22.08.03

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

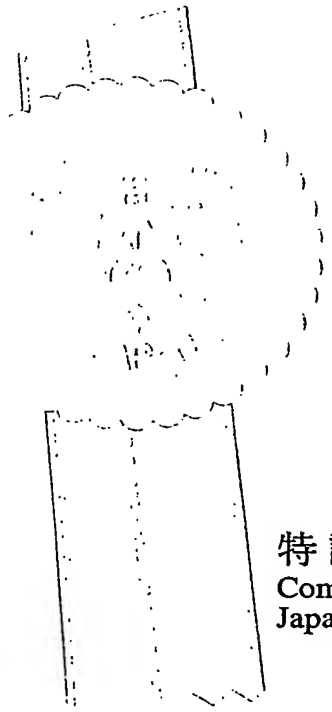
出願年月日
Date of Application: ２００２年　９月２５日

出願番号
Application Number: 特願２００２－２７８４３６

[ST. 10/C]: ［Ｊ Ｐ ２００２－２７８４３６］

出願人
Applicant(s): ソニー株式会社

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)



２００３年　９月２６日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

出証番号　出証特２００３－３０７９２３６

【書類名】　特許願
【整理番号】　0290539407
【提出日】　平成14年 9月25日
【あて先】　特許庁長官殿
【国際特許分類】　E05B 49/00
G08B 23/00
【発明者】
【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
【氏名】　油井　康二
【発明者】
【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
【氏名】　松村　広幸
【発明者】
【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
【氏名】　八重樫　章
【特許出願人】
【識別番号】　000002185
【氏名又は名称】　ソニー株式会社
【代理人】
【識別番号】　100091546
【弁理士】
【氏名又は名称】　佐藤　正美
【電話番号】　03-5386-1775
【手数料の表示】
【予納台帳番号】　048851
【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9710846

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　通信装置、通信システム、制御装置および認証装置

【特許請求の範囲】

【請求項１】

同一のものが存在しないように一元管理されて割り振られた識別情報を記憶する記憶部と、

ドアの施錠、開錠を行なうためのドアロック機構を制御するための制御装置との通信を行なう通信部と、

前記通信部を介して、前記記憶部の前記識別情報を、前記ドアの施錠、開錠を制御するための電子鍵情報として、前記制御装置に送信するように制御する制御部と、

を備える通信装置。

【請求項２】

ＩＣ（Ｉｎｔｅｇｒａｔｅｄ　Ｃｉｒｃｕｉｔ；集積回路）カードからなることを特徴とする請求項１に記載の通信装置。

【請求項３】

前記制御装置との通信機能ではない主たる別機能を備える電子機器からなることを特徴とする請求項１に記載の通信装置。

【請求項４】

電子鍵情報に応じてドアの施錠、開錠を行なうためのドアロック機構を制御する制御装置と、前記制御装置に前記電子鍵情報を送信する通信装置とからなる通信システムであって、

前記通信装置は、

同一のものが存在しないように一元管理されて割り振られた識別情報を記憶する第１の記憶部と、

前記制御装置との通信を行なうための第１の通信部と、

前記第１の通信部を介して、前記第１の記憶部の前記識別情報を、前記ドアの施錠、開錠を制御するための電子鍵情報として、前記制御装置に送信するように制御する第１の制御部と、

を備え

前記制御装置は、

前記通信装置と通信を行なうための第２の通信部と、

前記識別情報を前記電子鍵情報として記憶する第２の記憶部と、

前記第２の記憶部に前記識別情報を前記電子鍵情報として登録するための登録手段と、

前記第２の通信部を通じて前記通信装置から受信した前記識別情報と、前記第２の記憶部に記憶されている識別情報とを比較し、その比較結果に基づいて前記ドアの施錠、開錠を制御する第２の制御部と、

を備えることを特徴とする通信システム。

【請求項５】

請求項４に記載の通信システムにおいて、

前記制御装置の前記第２の記憶部には、前記電子鍵情報としての前記識別情報は、複数個、登録されて記憶可能とされる

ことを特徴とする通信システム。

【請求項６】

請求項５に記載の通信システムにおいて、

前記複数個の識別情報は、本鍵情報と、バックアップ鍵情報とからなる

ことを特徴とする通信システム。

【請求項７】

請求項６に記載の通信システムにおいて、

前記第２の制御部は、前記第２の通信部を通じて前記通信装置から受信した前記識別情報と、前記第２の記憶部に記憶されている前記本鍵情報としての識別情報とを比較し、その比較結果に基づいて前記ドアの施錠、開錠を制御する

ことを特徴とする通信システム。

【請求項８】

請求項７に記載の通信システムにおいて、

前記制御装置は、前記第２の記憶部の前記本鍵情報として登録されている識別情報が抹消されたときに、前記バックアップ鍵情報として登録されている識別情

報を本鍵情報として扱う

ことを特徴とする通信システム。

【請求項９】

請求項６に記載の通信システムにおいて、

前記第２の制御部は、前記第２の通信部を通じて前記通信装置から受信した前記識別情報と、前記第２の記憶部に記憶されている前記本鍵情報および前記バックアップ鍵情報としての識別情報とを比較し、その比較結果に基づいて前記ドアの施錠、開錠を制御する

ことを特徴とする通信システム。

【請求項１０】

電子鍵情報に応じてドアの施錠、開錠を行なうためのドアロック機構を制御するドアロック制御装置と、前記電子鍵情報の認証を行なう認証装置と、前記電子鍵情報を前記ドアロック制御装置または前記認証装置に送信する通信装置とからなる通信システムであって、

前記通信装置は、

同一のものが存在しないように一元管理されて割り振られた識別情報を記憶する第１の記憶部と、

前記制御装置との通信を行なうための第１の通信部と、

前記通信部を介して、前記記憶部の前記識別情報を、前記ドアの施錠、開錠を制御するための電子鍵情報として、前記制御装置に送信するように制御する第１の制御部と、

を備え

前記ドアロック制御装置は、

前記通信装置と通信を行なうための第２の通信部と、

前記第２の通信部で受信した前記通信装置からの前記電子鍵情報としての前記識別情報を前記認証装置に転送する転送手段と、

前記認証装置からの前記電子鍵情報についての認証結果を受信する手段と、

前記受信した前記認証結果に基づいて、前記ドアの施錠、開錠を制御する第２の制御部と、

を備え、

前記認証装置は、

前記電子鍵情報としての前記識別情報を記憶する第２の記憶部と、

前記第２の記憶部に前記識別情報を電子鍵情報として記憶して登録するための登録手段と、

前記ドアロック制御装置から転送されてくる前記識別情報と、前記第２の記憶部に記憶されている識別情報とを比較し、その比較結果を前記電子鍵情報の認証結果として前記ドアロック制御装置に送る手段と、

を備えることを特徴とする通信システム。

【請求項１１】

請求項１０に記載の通信システムにおいて、

前記認証装置の前記登録手段は、前記転送手段により前記ドアロック制御装置から送られてくる識別情報を、前記電子鍵情報として前記第２の記憶部に記憶して登録する

ことを特徴とする通信システム。

【請求項１２】

請求項１０に記載の通信システムにおいて、

前記認証装置は、さらに前記通信装置と通信を行なうための第３の通信部を備え、

前記認証装置の前記登録手段は、前記第３の通信部を通じて前記通信装置から送られてくる識別情報を、前記電子鍵情報として前記第２の記憶部に記憶して登録する

ことを特徴とする通信システム。

【請求項１３】

請求項１０に記載の通信システムにおいて、

前記認証装置の前記第２の記憶部には、前記電子鍵情報としての前記識別情報は、複数個、登録されて記憶可能とされる

ことを特徴とする通信システム。

【請求項１４】

請求項１３に記載の通信システムにおいて、

前記複数個の識別情報は、本鍵情報と、バックアップ鍵情報とからなる

ことを特徴とする通信システム。

【請求項１５】

請求項１４に記載の通信システムにおいて、

前記認証装置では、前記ドアロック制御装置から受信した前記識別情報と、前記第２の記憶部に記憶されている前記本鍵情報としての識別情報とを比較し、その比較結果を認証結果とする

ことを特徴とする通信システム。

【請求項１６】

請求項１５に記載の通信システムにおいて、

前記認証装置は、前記第２の記憶部の前記本鍵情報として登録されている識別情報が抹消されたときに、前記バックアップ鍵情報として登録されている識別情報を本鍵情報として扱う

ことを特徴とする通信システム。

【請求項１７】

請求項１４に記載の通信システムにおいて、

前記認証装置は、前記ドアロック制御装置から受信した前記識別情報と、前記第２の記憶部に記憶されている前記本鍵情報および前記バックアップ鍵情報としての識別情報とを比較し、その比較結果を認証結果とする

ことを特徴とする通信システム。

【請求項１８】

同一のものが存在しないように一元管理されて割り振られた識別情報を、電子鍵情報として記憶するための記憶部と、

前記識別情報を受信するための通信部と、

前記記憶部に前記識別情報を前記電子鍵情報として登録するための登録手段と、

前記通信部を通じて受信した前記識別情報と、前記第２の記憶部に記憶されている識別情報とを比較し、その比較結果に基づいてドアの施錠、開錠を制御する

制御部と、

を備えることを特徴とする制御装置。

【請求項１９】

請求項１８に記載の制御装置において、

前記記憶部には、前記電子鍵情報としての前記識別情報は、複数個、登録されて記憶可能とされる

ことを特徴とする制御装置。

【請求項２０】

請求項１９に記載の制御装置において、

前記複数個の識別情報は、本鍵情報と、バックアップ鍵情報とからなる

ことを特徴とする制御装置。

【請求項２１】

請求項２０に記載の制御装置において、

前記制御部は、前記通信部を通じて受信した前記識別情報と、前記記憶部に記憶されている前記本鍵情報としての識別情報とを比較し、その比較結果に基づいて前記ドアの施錠、開錠を制御する

ことを特徴とする制御装置。

【請求項２２】

請求項２１に記載の制御装置において、

前記記憶部の前記本鍵情報として登録されている識別情報が抹消されたときに、前記バックアップ鍵情報として登録されている識別情報を本鍵情報として扱う

ことを特徴とする制御装置。

【請求項２３】

請求項２０に記載の制御装置において、

前記制御部は、前記通信部を通じて受信した前記識別情報と、前記記憶部に記憶されている前記本鍵情報および前記バックアップ鍵情報としての識別情報とを比較し、その比較結果に基づいて前記ドアの施錠、開錠を制御する

ことを特徴とする制御装置。

【請求項２４】

同一のものが存在しないように一元管理されて割り振られた識別情報を電子鍵情報として記憶する記憶部と、

前記記憶部に前記識別情報を電子鍵情報として記憶して登録するための登録手段と、

ドアの施錠、開錠を制御するようにする制御装置から送られてくる前記識別情報を受信する受信手段と、

前記受信手段で受信した前記制御装置から送られてくる前記識別情報と、前記第２の記憶部に記憶されている識別情報とを比較し、その比較結果を前記電子鍵情報の認証結果として前記制御装置に送る手段と、

を備えることを特徴とする認証装置。

【請求項２５】

請求項２４に記載の認証装置において、

前記登録手段は、前記制御装置から送られてくる前記識別情報を、前記記憶部に記憶して前記電子鍵情報を登録する

ことを特徴とする認証装置。

【請求項２６】

請求項２４に記載の認証装置において、

前記識別情報を受信するための別の通信部を備え、

前記登録手段は、前記別の通信部を通じて受信する識別情報を、前記電子鍵情報として前記記憶部に記憶して登録する

ことを特徴とする認証装置。

【請求項２７】

請求項２４に記載の認証装置において、

前記記憶部には、前記電子鍵情報としての前記識別情報は、複数個、登録されて記憶可能とされる

ことを特徴とする認証装置。

【請求項２８】

請求項２４に記載の認証装置において、

前記記憶部には、前記電子鍵情報としての前記識別情報は、複数個、登録され

て記憶される

ことを特徴とする認証装置。

【請求項２９】

請求項２８に記載の認証装置において、

前記複数個の識別情報は、本鍵情報と、バックアップ鍵情報とからなる

ことを特徴とする認証装置。

【請求項３０】

請求項２９に記載の認証装置において、

前記制御装置から受信した前記識別情報と、前記記憶部に記憶されている前記本鍵情報としての識別情報とを比較し、その比較結果を認証結果とする

ことを特徴とする認証装置。

【請求項３１】

請求項３０に記載の認証装置において、

前記記憶部の前記本鍵情報として登録されている識別情報が抹消されたときに、前記バックアップ鍵情報として登録されている識別情報を本鍵情報として扱う

ことを特徴とする認証装置。

【請求項３２】

請求項２９に記載の認証装置において、

前記認証装置は、前記制御装置から受信した前記識別情報と、前記記憶部に記憶されている前記本鍵情報および前記バックアップ鍵情報としての識別情報とを比較し、その比較結果を認証結果とする

ことを特徴とする認証装置。

【請求項３３】

電子鍵情報に応じてドアの施錠、開錠を行なうためのドアロック機構を制御する制御装置と、前記制御装置に前記電子鍵情報を送信する通信装置と、前記電子鍵情報を管理するサーバ装置とからなる通信システムであって、

前記通信装置は、

同一のものが存在しないように一元管理されて割り振られた識別情報を記憶する第１の記憶部と、

前記制御装置との通信を行なうための第１の通信部と、

前記通信部を介して、前記記憶部の前記識別情報を、前記ドアの施錠、開錠を制御するための電子鍵情報として、前記制御装置に送信するように制御する第１の制御部と、

を備え、

前記制御装置は、

前記通信装置と通信を行なうための第２の通信部と、

前記サーバ装置と通信を行なうための第３の通信部と、

前記電子鍵情報としての前記識別情報を記憶する第２の記憶部と、

前記第３の通信部を通じて前記サーバ装置から受信した前記識別情報を前記第２の記憶部に前記電子鍵情報として記憶して登録するための登録手段と、

前記第２の通信部を通じて前記通信装置から受信した前記識別情報と、前記第２の記憶部に記憶されている識別情報とを比較し、その比較結果に基づいて前記ドアの施錠、開錠を制御する第２の制御部と、

を備え、

前記サーバ装置は、

前記通信装置の前記第１の記憶部に記憶されている識別情報を電子鍵情報として、前記制御装置を指定する情報とともに受信する受信手段と、

前記受信手段で受信した前記識別情報を、前記指定された前記制御装置の識別用情報と対応付けて記憶する第３の記憶部と、

前記受信手段で受信した前記識別情報を、前記指定された前記制御装置に転送する転送手段と、

を備えることを特徴とする通信システム。

【請求項３４】

請求項３３に記載の通信システムにおいて、

前記サーバ装置の第３の記憶部および前記制御装置の第２の記憶部には、前記電子鍵情報としての前記識別情報は、複数個、登録されて記憶可能とされる

ことを特徴とする通信システム。

【請求項３５】

請求項３４に記載の通信システムにおいて、

前記複数個の識別情報は、本鍵情報と、バックアップ鍵情報とからなる

ことを特徴とする通信システム。

【請求項３６】

請求項３５に記載の通信システムにおいて、

前記制御装置の前記第２の制御部は、前記第２の通信部を通じて前記通信装置から受信した前記識別情報と、前記第２の記憶部に記憶されている前記本鍵情報としての識別情報とを比較し、その比較結果に基づいて前記ドアの施錠、開錠を制御する

ことを特徴とする通信システム。

【請求項３７】

請求項３６に記載の通信システムにおいて、

前記制御装置は、前記サーバ装置からの本鍵情報の抹消登録要求を受けたときに、前記第２の記憶部の前記本鍵情報として登録されている識別情報を抹消し、前記バックアップ鍵情報として登録されている識別情報を本鍵情報として扱う

ことを特徴とする通信システム。

【請求項３８】

請求項３５に記載の通信システムにおいて、

前記制御装置の前記第２の制御部は、前記第２の通信部を通じて前記通信装置から受信した前記識別情報と、前記第２の記憶部に記憶されている前記本鍵情報および前記バックアップ鍵情報としての識別情報とを比較し、その比較結果に基づいて前記ドアの施錠、開錠を制御する

ことを特徴とする通信システム。

【請求項３９】

請求項３３に記載の通信システムにおいて、

前記制御装置と前記サーバ装置とは、通信ネットワークを通じて接続されており、前記サーバ装置には、複数の前記制御装置の前記ネットワーク上のアドレス情報が記憶されている

ことを特徴とする通信システム。

【請求項４０】

電子鍵情報に応じてドアの施錠、開錠を行なうためのドアロック機構を制御するドアロック制御装置と、前記電子鍵情報の認証を行なう認証装置と、前記電子鍵情報を前記ドアロック制御装置または前記認証装置に送信する通信装置と、前記電子鍵情報を管理するサーバ装置とからなる通信システムであって、

前記通信装置は、

同一のものが存在しないように一元管理されて割り振られた識別情報を記憶する第１の記憶部と、

前記制御装置との通信を行なうための第１の通信部と、

前記通信部を介して、前記記憶部の前記識別情報を、前記ドアの施錠、開錠を制御するための電子鍵情報として、前記制御装置に送信するように制御する第１の制御部と、

を備え

前記ドアロック制御装置は、

前記通信装置と通信を行なうための第２の通信部と、

前記第２の通信部で受信した前記通信装置からの前記電子鍵情報としての前記識別情報を前記認証装置に転送する転送手段と、

前記認証装置からの前記電子鍵情報についての認証結果を受信する手段と、

前記受信した前記認証結果に基づいて、前記ドアの施錠、開錠を制御する第２の制御部と、

を備え、

前記認証装置は、

前記電子鍵情報としての前記識別情報を記憶する第２の記憶部と、

前記サーバ装置と通信を行なうための第３の通信部と、

前記第３の通信部を通じて前記サーバ装置から受信した前記識別情報を前記第２の記憶部に電子鍵情報として記憶して登録するための登録手段と、

前記ドアロック制御装置から転送されてくる前記識別情報と、前記第２の記憶部に記憶されている識別情報とを比較し、その比較結果を前記電子鍵情報の認証結果として前記ドアロック制御装置に送る手段と、

を備え、

前記サーバ装置は、

前記通信装置の前記第１の記憶部に記憶されている識別情報を電子鍵情報として、前記制御装置を指定する情報とともに受信する受信手段と、

前記受信手段で受信した前記識別情報を、前記指定された前記認証装置の識別用情報と対応付けて記憶する第３の記憶部と、

前記受信手段で受信した前記識別情報を、前記指定された前記認証装置に転送する転送手段と、

を備えることを特徴とする通信システム。

【請求項４１】

請求項４０に記載の通信システムにおいて、

前記認証装置の前記第２の記憶部には、前記電子鍵情報としての前記識別情報は、複数個、登録されて記憶可能とされる

ことを特徴とする通信システム。

【請求項４２】

請求項４１に記載の通信システムにおいて、

前記複数個の識別情報は、本鍵情報と、バックアップ鍵情報とからなる

ことを特徴とする通信システム。

【請求項４３】

請求項４２に記載の通信システムにおいて、

前記認証装置では、前記ドアロック制御装置から受信した前記識別情報と、前記第２の記憶部に記憶されている前記本鍵情報としての識別情報とを比較し、その比較結果を認証結果とする

ことを特徴とする通信システム。

【請求項４４】

請求項４３に記載の通信システムにおいて、

前記認証装置は、前記サーバ装置からの本鍵情報の抹消登録要求を受けたときに、前記第２の記憶部の前記本鍵情報として登録されている識別情報を抹消し、前記バックアップ鍵情報として登録されている識別情報を本鍵情報として扱う

ことを特徴とする通信システム。

【請求項４５】

請求項４２に記載の通信システムにおいて、

前記認証装置は、前記ドアロック制御装置から受信した前記識別情報と、前記第２の記憶部に記憶されている前記本鍵情報および前記バックアップ鍵情報としての識別情報とを比較し、その比較結果を認証結果とする

ことを特徴とする通信システム。

【請求項４６】

請求項４に記載の通信システムにおいて、

前記制御装置の前記第２の記憶部には、前記電子鍵情報は、個人情報と関連して記憶され、前記電子鍵情報は、個人識別情報としても用いられることを特徴とする通信システム。

【請求項４７】

請求項１０に記載の通信システムにおいて、

前記認証装置の前記第２の記憶部には、前記電子鍵情報は、個人情報と関連して記憶され、前記電子鍵情報は、個人識別情報としても用いられることを特徴とする通信システム。

【請求項４８】

請求項１８に記載の制御装置において、

前記記憶部には、前記電子鍵情報は、個人情報と関連して記憶され、前記電子鍵情報は、個人識別情報としても用いられることを特徴とする制御装置。

【請求項４９】

請求項２４に記載の認証装置において、

前記記憶部には、前記電子鍵情報は、個人情報と関連して記憶され、前記電子鍵情報は、個人識別情報としても用いられることを特徴とする認証装置。

【請求項５０】

請求項３３に記載の通信システムにおいて、

前記サーバ装置の第３の記憶部には、前記識別情報は個人情報と関連して記憶されると共に、前記制御装置の第２の記憶部においても、前記電子鍵情報として

の前記識別情報は個人情報と関連して記憶され、前記電子鍵情報は、個人識別情報としても用いられることを特徴とする通信システム。

【請求項５１】

請求項４０に記載の通信システムにおいて、

前記サーバ装置の第３の記憶部には、前記識別情報は個人情報と関連して記憶されると共に、前記認証装置の第２の記憶部においても、前記電子鍵情報としての前記識別情報は個人情報と関連して記憶され、前記電子鍵情報は、個人識別情報としても用いられることを特徴とする通信システム。

【請求項５２】

請求項１８に記載の制御装置において、

前記電子鍵情報を管理するサーバ装置と通信する通信手段を備え、

前記登録手段は、前記通信手段を通じて取得した前記識別情報を前記電子鍵情報として前記記憶部に記憶することを特徴とする制御装置。

【請求項５３】

請求項２４に記載の認証装置において、

前記電子鍵情報を管理するサーバ装置と通信する通信手段を備え、

前記登録手段は、前記通信手段を通じて取得した前記識別情報を前記電子鍵情報として前記記憶部に記憶することを特徴とする認証装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

この発明は、電子鍵情報を用いてドアの施錠、開錠を制御するようにするドアロックシステムに用いて好適な通信装置および通信システムに関する。

【０００２】

【従来の技術】

従来の物理的な鍵を鍵シリンダーに差し込んで施錠、開錠を行なうドアロックシステムにおいては、鍵を紛失した場合には、ドアロック機構の鍵シリンダーを当該鍵以外の鍵を用いるものに交換しない限り、悪意の紛失鍵の拾得者にドアが開錠されてしまうおそれがつきまとう。また、最近は、鍵シリンダー機構に精通

しているものが、鍵を用いずに開錠することによる盗難等の事件が発生している。

【０００３】

そこで、このような鍵シリンダー機構を用いない電子鍵によるドアロックシステムが注目されている。例えば、この電子鍵によるドアロックシステムの一例として、親機は、予め登録されているＩＤコードと、電子鍵としての子機から受信したＩＤコードを比較照合して、その比較結果に基づいてドアロックをコントロールするものが知られている（例えば特許文献１参照）。

【０００４】

【特許文献１】

特開平９－４２９３号公報。

【０００５】

【発明が解決しようとする課題】

ところで、鍵を用いるシステムにおいては、鍵の紛失を考慮していわゆるスペア鍵を用意することが一般的に行なわれる。これは、電子鍵においても同様であり、通常は、鍵を複製してスペア鍵を作る。したがって、複数の同一鍵が用意されることになる。

【０００６】

しかし、同一の鍵が複数になることは、それだけ鍵の紛失の機会も増えることになり、セキュリティ上、好ましくない。また、ＩＤコードなどの識別情報を電子鍵情報として用いる場合に、たまたま同じＩＤコードが異なる電子鍵に登録されてしまうと、同様に、セキュリティ上、好ましくない。

【０００７】

この発明は、以上の問題点を解決することができる通信装置および通信システムを提供することを目的とする。

【０００８】

【課題を解決するための手段】

上記課題を解決するために、請求項１の発明による通信装置は、

同一のものが存在しないように一元管理されて割り振られた識別情報を記憶す

る記憶部と、

ドアの施錠、開錠を行なうためのドアロック機構を制御するための制御装置との通信を行なう通信部と、

前記通信部を介して、前記記憶部の前記識別情報を、前記ドアの施錠、開錠を制御するための電子鍵情報として、前記制御装置に送信するように制御する制御部と、

を備えることを特徴とする。

【０００９】

この請求項１の発明によれば、電子鍵として使用される識別情報は、同一のものが存在しないように一元管理されており、各通信装置には、異なる識別情報が記憶されることになる。したがって、この識別情報が電子鍵情報として用いられれば、セキュリティ上、好ましい。

【００１０】

請求項４の発明による通信システムは、

電子鍵情報に応じてドアの施錠、開錠を行なうためのドアロック機構を制御する制御装置と、前記制御装置に前記電子鍵情報を送信する通信装置とからなる通信システムであって、

前記通信装置は、

同一のものが存在しないように一元管理されて割り振られた識別情報を記憶する第１の記憶部と、

前記制御装置との通信を行なうための第１の通信部と、

前記第１の通信部を介して、前記第１の記憶部の前記識別情報を、前記ドアの施錠、開錠を制御するための電子鍵情報として、前記制御装置に送信するように制御する第１の制御部と、

を備え

前記制御装置は、

前記通信装置と通信を行なうための第２の通信部と、

前記電子鍵情報としての前記識別情報を記憶する第２の記憶部と、

前記第２の記憶部に前記識別情報を前記電子鍵情報として登録するための登録

手段と、

前記第２の通信部を通じて前記通信装置から受信した前記識別情報と、前記第２の記憶部に記憶されている識別情報とを比較し、その比較結果に基づいて前記ドアの施錠、開錠を制御する第２の制御部と、

を備えることを特徴とする。

【００１１】

この請求項４の通信システムにおいては、ドアの施錠、開錠を制御する制御装置の第２の記憶部には、同一のものが存在しないように一元管理されて割り振られた識別情報が電子鍵情報として記憶されている。そして、制御装置の第２の制御部は、通信装置から受信した識別情報と、第２の記憶部に記憶されている識別情報とを比較し、その比較結果に応じて、ドアの施錠、開錠を制御する。

【００１２】

したがって、この請求項４の通信システムによれば、同一の電子鍵情報が複数個存在することはないから、セキュリティ上、非常に好ましい。そして、スペア鍵が必要とされる場合には、請求項５の通信システムのように、制御装置の第２の記憶部に、複数の電子鍵情報を登録しておけばよい。

【００１３】

【発明の実施の形態】

以下、この発明による通信装置および通信システムの実施形態を、図を参照しながら説明する。

【００１４】

以下に説明する例では、家の玄関ドアには通信装置の例としての電子鍵装置からの電子鍵情報を受信してドアの施錠、開錠を制御するドアロック制御システムを設け、また、家の中には、窓や玄関ドアからの賊の侵入、火災の発生、ガス漏れを検知して、それぞれの異常事態に対応する措置を取るセキュリティ監視システムを設け、このセキュリティ監視システムとドアロック制御システムとを、通信可能に接続して連動させて動作させるようにしている。そして、さらに、この例では、セキュリティ監視システムは、通信ネットワークを通じて管理サーバに接続して、全体として、実施形態の通信システムを構成している。

【００１５】

そして、電子鍵装置としては、種々の形態のものを使用可能であるが、この例では、制御用ＩＣ（Ｉｎｔｅｇｒａｔｅｄ　Ｃｉｒｃｕｉｔ）と、通信手段とが埋め込まれた装置が用いられる。そして、この例では、この電子鍵装置の具体例としては、ＩＣカード（以下、電子鍵装置という）の他、携帯電話端末、ＰＤＡ（Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ　Ａｓｓｉｓｔａｎｔｓ）端末などが用いられる。

【００１６】

すなわち、この例では、電子鍵装置として、電子鍵装置のみでなく、携帯電話端末やＰＤＡ端末なども使用可能とされる。通常は、本鍵装置としてＩＣカードが用いられ、携帯電話端末やＰＤＡ端末などはバックアップ端末（スペア）として用いられるようにされる。

【００１７】

この場合に、この実施形態では、各電子鍵装置に搭載される制御用ＩＣはメモリを備え、そのメモリには、同一のものが存在しないように一元管理された識別情報が記憶される。この例では、この識別情報としては、ＩＣチップ製造番号が用いられる。

【００１８】

例えば、図１に示すように、１社あるいは複数社のＩＣチップの製造会社１００１において、製造した制御用ＩＣチップ１００２に対して、一元管理された重複のないＩＣチップ製造番号を付与するようにする。ＩＣチップの製造会社１００１が複数社の場合には、例えば、それぞれのＩＣチップ製造会社１００１に、予め、制御用ＩＣチップ１００２に付与する製造番号を割り当てておくようにすることにより、一元管理される。したがって、製造された制御用ＩＣチップ１００２のメモリには、互いに異なるＩＣチップ製造番号が識別情報として記憶される。

【００１９】

この制御用ＩＣチップ１００２は、ＩＣカード製造工場（あるいは製造会社）１００３、携帯電話端末製造工場（あるいは製造会社）１００４、ＰＤＡ端末製

造工場（あるいは製造会社）１００５などに供給されて、それらの制御用ＩＣチップと通信手段とが搭載されたＩＣカード、携帯電話端末、ＰＤＡ端末などが製造される。

【００２０】

図２は、この実施形態で用いられるＩＣチップ製造番号の一例を説明するための図である。

【００２１】

この例のＩＣチップ製造番号は、３桁のメーカー番号と、３桁のカテゴリーコードと、４桁のシリアル番号とからなる、合計１０桁の番号（記号を含む）で構成される。

【００２２】

なお、識別情報は、ＩＣチップ製造番号の限定されるものではなく、同一のものが存在しないように一元管理された情報であれば、どのようなものも使用可能である。また、識別情報は、ＩＣチップ製造番号と共に、別個にＩＣのメモリに記憶するようにしてもよい。

【００２３】

電子鍵装置の通信手段としては、電磁誘導や電波を用いた非接触による通信手段が用いられる。この実施形態においては、この通信手段は、例えば数ミリメートル～数十センチメートルの範囲で通信ができるものであればよく、小パワーのもので十分である。

【００２４】

次に、この実施形態の通信システムに用いられるドアロック制御システムにおいては、玄関ドアには、電子鍵装置によりドアの施錠、開錠を行なえるようにするためのドアロック装置が取り付けられる。この例では、電子鍵装置とドアロック装置との間では、鍵情報の通信を行ない、ドアロック装置は、その通信に基づいてドアの施錠、開錠を制御するようにする。

【００２５】

この例では、電子鍵装置とドアロック装置との間の通信は、以下に説明する例では、電磁誘導を用いた非接触による通信とされており、後述するように、ドア

ロック装置の一部を構成する電子鍵装置のリード／ライト部を介して、通信が行われる。

【００２６】

ドアの施錠、開錠を制御するための鍵情報としては、前述したＩＣチップ製造番号からなる識別情報が用いられる。当該家に住む住人（この明細書の説明では、簡単のため、家族構成員とする）の全員に共通の一つとして、各人が、その共通鍵情報を格納する電子鍵装置をそれぞれ持つようにすることもできるが、それでは、前述したような不具合が生じるおそれがある。

【００２７】

そこで、この実施形態では、当該家における電子鍵情報として、前述のようにして一元管理された識別情報が内蔵メモリに書き込まれた電子鍵装置の前記識別情報を電子鍵情報として管理サーバ装置に登録することにより、家族構成員のそれぞれが、自分用の電子鍵装置を所有して使用するようにする。

【００２８】

管理サーバ装置は、登録された家族構成員のそれぞれについての電子鍵情報をドアロック装置の電子鍵情報の記憶部に転送して、電子鍵情報をドアロック装置に登録させるようにする。ドアロック装置は、登録された電子鍵情報と、通信装置としての電子鍵装置から受信した電子鍵情報とを比較し認証して、その結果に応じてドアの施錠、開錠を制御する。

【００２９】

後述するように、この実施形態では、家族構成員のそれぞれは、自分用の電子鍵情報として、本鍵情報と、バックアップ鍵情報とを管理サーバ装置に登録することができる。電子鍵情報は、前述したように、電子鍵装置ごとに異なるので、本鍵情報とバックアップ鍵情報との登録は、本鍵装置と、バックアップ鍵装置との登録に等しい。

【００３０】

この実施形態では、本鍵装置としては、ドアロック制御システムの提供会社が提供するＩＣカードとされる。そして、この本鍵装置であるＩＣカードの識別情報が、ドアロック制御システムが当該家に取り付けられる前に、予め管理サーバ

装置に電子鍵情報として登録される。

【００３１】

この場合に、この実施形態では、家族構成員の数分だけ、ＩＣカードが前記提供会社から提供され、それらの複数のＩＣカードの全ての識別情報が、設置されるドアロック制御システム用の電子鍵情報として管理サーバ装置に登録される。

【００３２】

さらに、この実施形態では、管理サーバ装置には、ドアロック制御システムが設置される家の家族構成員のそれぞれについての個人情報が収集され、その個人情報に対応して、それぞれの家族構成員が持つＩＣカードの識別情報が登録される。したがって、ドアロック制御システムは、電子鍵情報を検索することにより、それが誰の電子鍵情報であるかを判別することができる。つまり、この例の通信システムにおいては、電子鍵情報を、家族構成員の個人識別情報として用いることが可能である。

【００３３】

そして、管理サーバ装置に登録された各家族構成員の本鍵情報は、ドアロック制御システムが、当該家に設置された後、システムの設置事業者や、ユーザが管理サーバ装置に対して初期登録要求をすることにより、ドアロック装置の記憶部に登録され、電子鍵情報の認証用として使用されることになる。

【００３４】

また、この実施形態では、本鍵装置を紛失してしまった場合を考慮して、バックアップ鍵情報を登録しておくことができる。後述するように、この実施形態では、バックアップ鍵情報は、家族構成員の各人が、バックアップ鍵装置として使用したい電子鍵装置の識別情報（この例では、ＩＣ製造番号）を管理サーバ装置に登録することにより、登録可能である。

【００３５】

なお、本鍵情報とバックアップ鍵情報との電子鍵情報の認証についての取り扱い方法としては、本鍵情報とバックアップ鍵情報とを同等に扱う方法と、認証用としては本鍵情報のみを原則とし、本鍵情報が抹消されたときに、バックアップ鍵情報が登録されていれば、以後は、バックアップ鍵情報を本鍵情報として取り

扱うようにする方法とがある。いずれの方法を用いることができるが、できるだけ、認証用としては、少ない方がセキュリティ上は好ましいと考えられるので、この実施形態では、後者の場合を採用するものとしている。

【００３６】

前述したように、この実施形態においては、電子鍵情報として用いる識別情報は、個人識別情報としても用いることができることを利用して、各家族構成員個々の玄関ドアからの入退出を管理することができるようにする。

【００３７】

このように電子鍵情報を個人識別情報としても用いることにより、当該家に住む家族構成員それぞれの玄関ドアからの入退出の管理情報を、セキュリティシステムに反映させることができ、より高機能のセキュリティシステムを構築することができる。

【００３８】

[実施形態のドアロックシステムを含むセキュリティシステムの概要]

図３は、ドアロック制御システムおよびセキュリティシステムを含む、この実施形態の通信システムの概要を説明するための図である。

【００３９】

家の玄関ドア１には、電子鍵装置と通信を行なうドアロック装置２が取り付けられている。室内には、セキュリティシステムを構成する監視制御装置３が設けられ、ドアロック装置２と接続されている。ドアロック装置２と監視制御装置３とは、この例では接続線により接続されるが、無線により接続するようにしてもよい。

【００４０】

監視制御装置３は、ドアロック装置２からの電子鍵情報を受け取って、前述した電子鍵情報の認証を行なう装置、つまり認証装置となることもできる。しかし、この例では、電子鍵情報の認証は、ドアロック装置２自身において行なうようにされている。

【００４１】

そして、この例では、室内には、火災発生を検知する火災センサ４と、ガス漏

れを検知するガスセンサ５と、窓の戸締りを検知する窓センサ６ａ，６ｂと、テレビ７が設けられ、それぞれ監視制御装置３に接続されている。監視制御装置３とそれらとの接続も、接続線により接続されているが、無線により接続してもよい。

【００４２】

また、図３では省略したが、火災センサ４で火災発生を検知したときに、その発生現場近傍を撮影できるような位置や、窓センサ６ａ，６ｂで賊の侵入を検知したときに、その賊を撮影できるような位置には、監視カメラを設けるようにすることができる。その場合には、それら監視カメラは監視制御装置３に接続され、監視カメラの撮影画像が監視制御装置３に供給されるようにされる。

【００４３】

監視制御装置３は、また、電話回線８を通じ、通信ネットワーク９を通じてセキュリティシステムの管理会社が運営する管理サーバ装置１０に接続される。この管理サーバ装置１０も、ドアロック装置２からの電子鍵情報を、監視制御装置３を介して受け取ることにより、電子鍵情報の認証を行なう装置となることもできる。

【００４４】

通信ネットワーク９は、携帯電話網をも含み、後述するように、監視制御装置３は、異常状態の発生時に、予め登録された携帯電話端末１１ａ，１１ｂに、当該異常状態の発生を知らせることが可能とされている。さらに、通信ネットワーク９は、インターネットを含み、パーソナルコンピュータ１２は、管理サーバ装置１０に対して当該インターネットを通じてアクセスすることが可能とされている。また、携帯電話端末１１ａ，１１ｂからも、管理サーバ装置１０にアクセスすることが可能とされている。

【００４５】

次に、ドアロック装置２の具体的構成例およびその動作、また、監視制御装置３の具体的構成例およびその動作について、詳細に説明する。なお、以下に説明する例では、前述したように、電子鍵情報の認証は、ドアロック装置自身が行なうものとする。

【００４６】

［ドアロック装置の構成］

図４（Ａ）および図４（Ｂ）は、ドアロック装置２の構成例を説明するための図である。図４（Ａ）は、家の外側から玄関ドア１のドアロック装置２の取り付け部分近傍を見た図である。また、図４（Ｂ）は、玄関ドア１のドアロック装置２の取り付け部分近傍を、玄関ドア１の端面側から見た図である。

【００４７】

この例のドアロック装置２においては、玄関ドア１の外側（戸外側）には、電子鍵装置と通信を行なうための外側電子鍵リーダ／ライタ部２１ｅｘと、電子鍵情報の認証結果や玄関ドア１の施錠または開錠を視覚的に知らせるための表示素子の例としての外側ＬＥＤ（Ｌｉｇｈｔ　Ｅｍｉｔｔｉｎｇ　Ｄｉｏｄｅ；発光ダイオード）２２ｅｘと、電子鍵情報の認証結果や玄関ドア１の施錠または開錠を音声により知らせるための外側スピーカ２３ｅｘと、外側ドアノブ２４ｅｘとが設けられている。

【００４８】

また、玄関ドア１の内側（屋内側）にも、電子鍵装置と通信を行なうための内側電子鍵リーダ／ライタ部２１ｉｎと、電子鍵情報の認証結果や玄関ドア１の施錠または開錠を視覚的に知らせるための表示素子の例としての内側ＬＥＤ２２ｉｎと、電子鍵情報の認証結果や玄関ドア１の施錠または開錠を音声により知らせるための内側スピーカ２３ｉｎと、内側ドアノブ２４ｉｎとが設けられている。

【００４９】

玄関ドア１には、さらに、玄関ドア係止片２５と、ロック片２６と、ドア開閉センサ２７が設けられている。さらに、玄関ドア１の内側には、ドアロック装置２の動作を制御するためのドアロック制御装置１００が設けられており、電子鍵リーダ／ライタ部２１ｅｘおよび２１ｉｎ、ＬＥＤ２２ｅｘおよび２２ｉｎ、スピーカ２３ｅｘおよび２３ｉｎ、ドア開閉センサ２７および図示を省略したドアロック機構駆動部が、このドアロック制御装置１００に接続されている。

【００５０】

玄関ドア係止片２５は、ドアノブ２４ｅｘあるいはドアノブ２４ｉｎの操作に

応じて、玄関ドアの端面１ａに垂直な方向に摺動移動する部材である。これは、後述するオートロックモードでない場合において、玄関ドア１が施錠されていないときにも、玄関ドア１の端面１ａと対向する壁の端面側に設けられる凹部に勘合して、玄関ドア１を、係止するためのものである。

【００５１】

ロック片２６は、ドアロック機構の一部を構成する部材であり、図４では図示を省略したドアロック機構駆動部によりドアロック機構が駆動されることにより、玄関ドアの端面１ａに垂直な方向に摺動移動して、玄関ドア１を施錠するときには、図４のように、玄関ドア１の端面１ａから突出する状態に固定され、玄関ドア１を開錠するときには、玄関ドア１の端面１ａから突出しない状態に固定される。

【００５２】

なお、図示は省略したが、玄関ドア１の端面１ａと対向する壁の端面には、このロック片２６が突出した状態のときに嵌合される凹部が形成されており、ロック片２６が当該凹部に嵌合される状態が玄関ドアの施錠状態となる。そして、ロック片２６が玄関ドア１側に引っ込んで、当該凹部に嵌合していないときには、施錠状態が解除されて、開錠状態になる。

【００５３】

玄関ドア開閉センサ２７は、例えば光学式センサが用いられ、玄関ドア１が開けられたときは外部光を検知することにより、それを検知し、玄関ドア１が閉じられたときには、玄関ドア１の端面１ａが、壁の端面と衝合することにより外部光が遮断されることを検知することにより、それを検知して、玄関ドア１の開閉を検知する。

【００５４】

［ドアロック制御装置１００の説明］

次に、ドアロック制御装置１００を中心にしたドアロック装置２の電気的な構成例を図５に示す。

【００５５】

すなわち、ドアロック制御装置１００は、マイクロコンピュータの構成を備え

ており、ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）１０１に対してシステムバス１０２を介してプログラムやデータが記録されているＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）１０３と、ワークエリア用ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）１０４と、家族構成員の個々についての電子鍵情報となる識別情報（この例では、ＩＣ製造番号）が記憶されている家族情報メモリ１２０と、監視制御装置３と通信を行なうための通信インターフェース１２１とが接続されている。

【００５６】

家族情報メモリ１２０には、後述するように、管理サーバ装置１０に登録された本鍵情報やバックアップ鍵情報が、家族構成員のそれぞれについて、電子鍵情報として登録されて格納されている。また、各家族構成員を識別するための情報、例えば、氏名、年齢、性別、続き柄、その他の個人情報も、併せて家族情報メモリ１２０に格納するようにしてもよい。この家族情報メモリ１２０への電子鍵情報の登録に関しては、後述する。

【００５７】

また、システムバス１０２には、インターフェース１０５および１０６を介して内側電子鍵リード／ライト部２１ｉｎおよび外側電子鍵リード／ライト部２１ｅｘが接続され、また、内側ＬＥＤ駆動部１０７を介して内側ＬＥＤ２２ｉｎが接続され、外側ＬＥＤ駆動部１０８を介して外側ＬＥＤ２２ｅｘが接続され、さらに、音声出力インターフェース１０９を介して内側スピーカ２３ｉｎが接続され、音声インターフェース１１０を介して外側スピーカ２３ｅｘが接続される。

【００５８】

さらに、システムバス１０２には、インターフェース１１１を介してドア開閉センサ２７が接続されると共に、ドアロック機構駆動部１１２を介して、ロック片２６を摺動駆動させるドアロック機構２８が接続される。

【００５９】

電子鍵リード／ライト部２１ｅｘまたは２１ｉｎは、電子鍵装置４０と通信を行なう通信部を構成する。電子鍵リード／ライト部２１ｅｘまたは２１ｉｎは、この例では、電磁誘導アンテナおよび情報送受信部を含む。

【００６０】

この例のドアロック制御装置１００は、ドアロック制御モードとして、オートロックモードと、逐次ロックモードとの２通りの制御モードを備えている。

【００６１】

オートロックモードは、ドアロック制御装置１００が、電子鍵リード／ライト部２１ｅｘ，２１ｉｎを介して電子鍵装置４０と通信することに基づき玄関ドア１を開錠した後、所定時間後に自動的に玄関ドアを施錠状態にするモードである。オートロックモードにおいては、常に、内側と外側の電子鍵リード／ライト部２１ｅｘ，２１ｉｎの両方を用いるものとなる。

【００６２】

また、逐次ロックモードは、少なくとも玄関ドア１の外側の電子鍵リード／ライト部２１ｅｘを通じて電子鍵装置４０と通信することに基づき玄関ドアの施錠、開錠の状態を、そのときの状態とは逆の状態にするモードである。この逐次ロックモードにおいても、内側と外側の電子鍵リード／ライト部２１ｅｘ，２１ｉｎの両方を用いることができるが、内側は、別途のマニュアルの施錠手段により施錠するようにした場合には、外側の電子鍵リード／ライト部２１ｅｘを通じた電子鍵装置４０との通信のみにより、玄関ドアの施錠、開錠動作を行なわせるようにすることができる。この逐次ロックモードは、従来からの一般的な鍵による施錠、開錠の方法に合わせたモードである。

【００６３】

ドアロック装置２のドアロック制御モードをオートロックモードとするか、逐次ロックモードとするかの選択設定は、この例では、例えば、ドアロック装置２を取り付ける際に、後述するように、作業者により監視制御装置３を通じて行なわれる。

【００６４】

ドアロック装置２がいずれのドアロック制御モードに設定されているかの情報は、ドアロック制御装置１００内の図示を省略した不揮発性メモリに格納されており、ドアロック制御装置１００は、当該不揮発性メモリの記憶情報を参照することにより、自装置のドアロック制御モードが、オートロックモードか、逐次ロ

ックモードかを認識するものである。監視制御装置３を通じたドアロック制御モードの設定動作に関しては、後述する。

【００６５】

なお、ドアロック装置２のドアロック制御モードをオートロックモードとするか、逐次ロックモードとするかの選択設定は、監視制御装置３を通じて行なうのではなく、ドアロック装置２に直接的に行なうようにすることもできる。例えば、予め、ドアロック装置２の出荷時に、いずれのドアロック制御モードにするかの設定をドアロック装置２に行なっておくようにしても良い。また、ドアロック装置２に、ドアロック装置２の設置作業者が操作可能な入力操作手段、例えばディップスイッチ等を設けておき、当該入力操作手段を通じて、ドアロック制御モードの設定を行なうようにしてもよい。

【００６６】

［電子鍵装置４０の構成例］

前述したように、この実施形態においては、電子鍵装置４０としては、ＩＣカードの他、携帯電話端末やＰＤＡ端末なども用いることができる。しかし、電子鍵装置４０は、電子鍵情報用の制御用ＩＣチップと通信手段とを備える点では共通している。

【００６７】

図６は、電子鍵装置４０がＩＣカード４０Ｃである場合の構成例を示す図である。図６（Ａ）は、ＩＣカード４０Ｃの表面を示し、この表面には、所有者の氏名と、ＩＤ番号が表示されている。また、図６（Ｂ）は、ＩＣカード４０Ｃの内部構成例を示しており、ＩＣカード４０Ｃ内には、電子鍵リード／ライト部と通信を行なうための電磁誘導用のアンテナ４１と、制御用ＩＣ４２とが内蔵されている。

【００６８】

制御用ＩＣ４２内には、メモリを含み、前述したＩＣ製造番号からなる識別情報、所有者の氏名、住所の他、所有者のその他の必要な個人情報が記憶されている。この個人情報は、父親、母親、子供などの区別が可能なように構成されている。また、制御用ＩＣ４２内のメモリに、各所有者が行った電子鍵リード／ライ

ト部２１ｅｘまたは２１ｉｎとの通信の時刻や履歴（内側と外側のどちらの電子鍵リード／ライト部と通信したか情報を含む）や、各所有者の外出、帰宅の履歴などを書き込むようにされている。

【００６９】

なお、これらの履歴情報は、ドアロック制御装置１００の家族情報メモリ１２０や監視制御装置３の後述の家族情報メモリ２０５における各人に対応するエリアにも記憶されるものである。

【００７０】

図７は、ＩＣカード４０Ｃの内部ブロック構成を示すものである。ＣＰＵ４０１に対してシステムバス４０２を介してプログラムやデータが記録されているＲＯＭ４０３と、ワークエリア用ＲＡＭ４０４と、電子鍵情報となる識別情報（この例では、ＩＣ製造番号）が記憶されている識別情報メモリ４０５と、通信履歴メモリ４０６と、送受信インターフェース４０７とが接続されている。識別情報メモリ４０５には、使用者の個人情報をも記憶することが可能である。

【００７１】

送受信インターフェース４０７には、電磁誘導アンテナ４１に接続されている情報送受信回路４０８が接続されている。そして、識別情報メモリ４０５から読み出した識別情報を送受信インターフェース４０７、情報送受信回路４０８および電磁誘導アンテナ４１を通じて送出する。

【００７２】

また、電磁誘導アンテナ４１にて受信した情報を、情報送受信回路４０８および送受信インターフェース４０７を通じて取り込み、通信履歴メモリに書き込んだりする。

【００７３】

[監視制御装置３の外観の説明]

図８は、室内に設けられるセキュリティシステム用の監視制御装置３の構成を説明するための外観図であり、この監視制御装置３は、例えば赤外線や電波を用いたリモートコマンダ５０によりリモコン制御可能の構成とされている。

【００７４】

監視制御装置３の筐体３０には、ビデオカメラ３１が組み込まれている。このビデオカメラ３１は、この例では、実線位置の横置き状態と、点線位置の縦置き状態とのいずれの状態をも取れる機構により、筐体３０に対して取り付けられている。このビデオカメラ３１は、セキュリティモードがオンとされたときに、監視制御装置３からの指示により撮影を開始するようにされている。

【００７５】

また、ビデオカメラ３１による撮影方向は、ビデオカメラが首振り方向に調整可能な構造とされているので、その調整により変えられるようにされている。したがって、使用者は、セキュリティモードオンに先立ち、ビデオカメラ３１による撮影方向の調整を行なっておくことができる。

【００７６】

そして、筐体３０には、ビデオカメラ３１による撮影対象部を明るく照明するための撮影用ランプ３２が設けられている。また、筐体３０には、例えば遠赤外線を検知することにより人を検知する人感センサ３３が設けられている。監視制御装置３は、後述するように、セキュリティモードオンのときに人感センサ３３で人を検知したときには、賊の侵入であるとして検知し、撮影用ランプ３２をオンにすると共に、所定の通報先に撮影画像を送るようにする。

【００７７】

筐体３０には、また、マイクロホン３４とスピーカ３５とが設けられている。マイクロホン３４は、賊の声や賊侵入時の室内の臨場音を収音するためのものである。スピーカ３５は、侵入してきた賊を威嚇する音声を放音するためなどに用いられる。

【００７８】

筐体３０には、また、電子鍵リード／ライト部３６が設けられる。この電子鍵リード／ライト部３６は、この例では、伝言の記録、再生の際に用いられる。すなわち、この例においては、監視制御装置３は、伝言装置の役割もできるように構成されており、電子鍵リード／ライト部３６により、電子鍵装置を読み取らせた後、後述するようにリモートコマンダ５０の伝言記録ボタンを押すと、設定した相手（家族の誰か）に伝言が残すことができ、また、リモートコマンダ５０の

伝言再生ボタンを押すと、自分宛ての伝言を再生することができるようになっている。

【００７９】

この伝言が記録されているかどうかなどを知らせるため等の用途として、筐体３０には、複数個のＬＥＤ３７が設けられている。また、筐体３０には、さらに、リモートコマンダ５０からのリモコン信号の受信部３８が設けられる。

【００８０】

また、図５では図示を省略したが、監視制御装置３の背面パネルには、テレビ受像機７のビデオ入力端子に接続される映像出力端子が設けられている。そして、監視制御装置３には、テレビ受像機７の電源のオン・オフなどを制御するためのリモコン送信部３９が設けられている。

【００８１】

さらに、監視制御装置３は、火災センサ４、ガスセンサ５、窓センサ６ａ，６ｂ、さらには、監視カメラを接続するためのセンサハブを備えている。また、図３で説明したように、監視制御装置３は、電話回線を通じて、セキュリティシステムの管理会社が運営する管理サーバ装置１０にアクセスできるように構成されている。

【００８２】

[監視制御装置３の構成例]

監視制御装置３の内部構成および監視制御装置３と周辺機器との接続状態の構成例を図９に示す。

【００８３】

監視制御装置３は、マイクロコンピュータの構成を備えており、ＣＰＵ２０１に対して、システムバス２０２を介して、プログラムやデータが記録されているＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）２０３と、ワークエリア用ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）２０４と、ドアロック制御装置１００の家族情報メモリ１２０と同様に、電子鍵装置４０を所有する家族全員の電子鍵情報となる識別情報が記憶されている家族情報メモリ２０５と、ドアロック制御装置１００と通信を行なうためのドアロック装置通信インターフェース２

０６と、センサハブ２０７と、ビデオカメラ３１の撮影画像およびマイクロホン３４で収音した音声を記憶するための画像・音声メモリ２０８と、電話回線を通じて管理サーバ装置１０等と通信を行なうための通信インターフェース２０９とが接続されている。

【００８４】

また、システムバス２０２には、カメラインターフェース２１０を介してビデオカメラ３１が、インターフェース２１１を介して撮影用ランプ３２の照明機構３２０が、インターフェース２１２を介して人感センサ３３が、インターフェース２１４を介して電子鍵リード／ライト部３６が、インターフェース２１５を介してリモコン受信部３８が、インターフェース２１６を介してリモコン送信部３９が、音声入力インターフェース２１８を介してマイクロホン３４が、インターフェース２１９を介してＬＥＤ３７が、音声出力インターフェース２２０を介してスピーカ３５が、それぞれ接続されている。さらに、システムバス２０２は、ビデオ信号出力端子からなるテレビインターフェース２１７を介してテレビ受像機７に接続されている。

【００８５】

家族情報メモリ２０５は、例えばＥＥＰＲＯＭ（Ｅｌｅｃｔｒｉｃａｌｌｙ Ｅｒａｓａｂｌｅ　Ｐｒｏｇｒａｍｍａｂｌｅ　ＲＯＭ）で構成される。

【００８６】

家族情報メモリ２０５には、ドアロック制御装置１００の家族情報メモリ１２０と同様に、家族構成員のそれぞれについての識別情報と、個人情報とが格納されている。この明細書では、識別情報と個人情報とからなる情報を、個人プロファイル情報と呼ぶことにする。

【００８７】

図１０に、一人分の個人プロファイル情報の例を示す。図１０に示すように、個人プロファイル情報は、個人識別情報と個人情報とが対応付けられて記憶された情報である。この実施形態では、個人識別情報は、前述したように、電子鍵装置の各メモリに格納されている識別情報が用いられる。個人識別情報は個人情報と対応させることで、具体的に誰の識別情報であるかが判明する。この識別情報

は、電子鍵情報の役割を有することは前述した通りであり、図１０に示すように、電子鍵情報としては、本鍵情報とバックアップ鍵情報とが登録可能である。バックアップ鍵情報は、複数個、登録可能としてもよい。

【００８８】

図１０の例においては、個人情報としては、パスワード情報、氏名、住所、生年月日、年齢、続柄、登録日、銀行口座番号、電話番号、趣味／嗜好情報、家の玄関８からの入退出履歴情報、電子鍵登録・紛失履歴情報などが家族情報メモリ２０５に記憶される。

【００８９】

この例の入退出履歴情報には、外出時刻、帰宅時刻が記憶されるほか、外出中であるか、在宅であるかの在／不在フラグが含まれる。この入退出履歴情報は、監視制御装置３が玄関ドア７を通じての家族の入退出を管理するために用いられる。また、電子鍵登録・紛失履歴情報は、後述するように、管理サーバ装置１０からの電子鍵情報のバックアップ登録要求や抹消要求が到来して、バックアップ登録や抹消処理をしたときに、その日付、時刻とともに、バックアップ鍵情報や抹消した電子鍵情報を、バックアップ登録および抹消の区別をして記録しておくものである。

【００９０】

さらに、この例では、この家族情報メモリ２０５には、セキュリティモード用の情報も格納されている。すなわち、この例では、監視制御装置３では、家族構成員の在宅状況に応じて、セキュリティレベルを変更することが可能なように構成されている。図１１は、セキュリティレベルと家族構成員の在宅状況との関係を示すテーブルである。また、図１２は、セキュリティレベルとセキュリティ内容との対応を示すテーブルである。

【００９１】

図１２に示すように、この例においては、セキュリティレベルは、セキュリティレベルが高い方から順に、レベルＡ、レベルＢ、レベルＣ、レベルＤまであり、レベルＡにおいては、窓および玄関ドアの監視、火災やガス漏れの監視、ビデオカメラ３１による監視の全てを行ない、レベルＢでは、ビデオカメラ３１によ

る監視は行なわずに、窓および玄関ドアの監視および火災やガス漏れの監視を行ない、レベルＣでは、火災やガス漏れの監視のみを行ない、レベルＤでは、監視を行なわない、という内容である。

【００９２】

そして、図１１に示すように、家族構成員の在宅状況のそれぞれに対して各セキュリティレベルが割り付けられる。すなわち、この例では、父親が在宅の状況では、監視を行なわないレベルＤとされる。また、父親が不在であるが母親が在宅の状況では、火災やガス漏れの監視のみを行なうレベルＣとされる。また、子供のみが在宅の状況では、窓および玄関ドアの監視および火災やガス漏れの監視を行なうレベルＢとされる。そして、全員が不在である状況では、全ての監視を行なうレベルＡとされる。

【００９３】

監視制御装置３では、セキュリティモードをオンにするとき、また、セキュリティレベルを変更するとき、これら図１１、図１２のテーブルを参照し、在宅状況に応じてセキュリティレベルを決定するようにする。

【００９４】

図１１のセキュリティレベルと、家族構成員の在宅状況との関係は、予め設定しておくこともできるし、使用者が、例えばリモートコマンダ５０を用いて監視制御装置３に入力設定することにより、設定を変更することできるように構成されている。

【００９５】

なお、これら図１１、図１２のテーブル情報は、家族情報メモリ２０５ではなく、別のメモリに格納するようにしても良いことは言うまでもない。

【００９６】

ドアロック装置通信インターフェース２０６は、ドアロック制御装置１００に接続されている。センサハブ２０７には、火災センサ４、ガスセンサ５、窓センサ６ａ，６ｂおよび１個あるいは複数個の監視カメラ１３が接続される。

【００９７】

画像・音声メモリ２０８は、セキュリティモードがオンであるときに、ビデオ

カメラ３１で撮影した画像情報と、マイクロホン３４で収音した音声情報とをバッファリングする監視情報領域と、伝言として記録されている画像情報および音声情報を記憶する伝言情報領域とを備えている。また、監視情報領域には、監視カメラ１３用の画像記憶領域も設けられている。

【００９８】

監視情報領域は、この例では、所定時間、例えば３０秒分の画像情報および音声情報を、いわゆるリングバッファ形式で記憶する。なお、監視情報領域と伝言情報領域とは、別々のメモリの構成とすることも勿論できる。

【００９９】

通信インターフェース２０９は、この例では、ルータ６１に接続されている。ルータ６１は、ＡＤＳＬモデム６２、スプリッタ６３を通じて電話回線６５に接続されている。スプリッタ６３には、電話端末６４が接続される。

【０１００】

［リモートコマンダ５０の説明］

監視制御装置３用のリモートコマンダ５０は、図８に示すように、セキュリティボタン５１と、オフボタン５２と、伝言記録ボタン５３と、伝言再生ボタン５４と、メニューボタン５５と、上下左右の選択を行なう４個のキーとその中央の決定キーとからなるカーソルボタン５６とを備えて構成されている。

【０１０１】

メニュー項目としては、この例では、管理サーバ装置１０に対する電子鍵情報としての個人ＩＤの登録、ドアロック装置２のドアロック制御モードの設定、その他が、用意されており、それぞれのメニュー項目に対応する処理を実行するアプリケーションプログラムは、監視制御装置３のＲＯＭ２０３に格納されている。

【０１０２】

［管理サーバ装置１０の構成］

次に、管理サーバ装置１０の構成例を図１３に示す。管理サーバ装置１０は、コンピュータの構成を備えており、ＣＰＵ３０１に対して、システムバス３０２を介して、プログラムやデータが記録されているＲＯＭ３０３と、ワークエリア

用ＲＡＭ３０４と、ドアロック装置管理データベース３０５と、電子鍵登録・紛失履歴メモリ３０６と、インターネットなどの通信ネットワークを通じて通信を行なうための通信インターフェース３０７とが接続されている。また、システムバス３０２には、さらに、ホームページ用メモリ３０８と、画像・音声メモリ３０９とが接続されている。

【０１０３】

ドアロック装置管理データベース３０５には、ドアロック装置２のシリアル番号、ドアロック装置２が設置された住所、電話番号、ドアロック装置の利用者の氏名、登録された電子鍵情報など、ドアロック装置２の管理に必要な事項が格納されている。

【０１０４】

電子鍵登録・紛失履歴メモリ３０６には、各ドアロック装置２ごとに、電子鍵情報の登録と紛失の履歴が記憶される。ホームページ用メモリ３０８には、ホームページの各ページの表示情報が格納されており、ＣＰＵ３０１の指示に従い、必要がページの表示情報が、このメモリ３０８から読み出されて、通信インターフェース３０７を通じて通信ネットワークに送出される。

【０１０５】

画像・音声メモリ３０９は、後述するように、セキュリティ監視システムから送られてくる画像・音声情報を格納する。管理サーバ装置１０では、セキュリティ監視システムからの画像・音声をチェックして、警備会社に通知したり、ユーザの求めに応じて、画像・音声情報をホームページを通じて提供するようにする。

【０１０６】

次に、以上のような構成の通信システムにおける種々の動作について、以下に説明する。

【０１０７】

[監視制御装置３における伝言記録および伝言再生；図１４]

前述したように、この例の監視制御装置３は、電子鍵装置４０と、リモートコマンダ５０を用いて、特定の家人を指定して、伝言を記録しておくことができる

。伝言が監視制御装置３に記録されているときには、ＬＥＤ３７が点灯あるいは点滅して、その旨を知らせるようにしている。

【０１０８】

そして、監視制御装置３に、伝言が記録されている場合には、帰宅した家人が、自分の電子鍵装置を、この電子鍵リード／ライト部３６により読み取らせ、リモートコマンダ５０により伝言再生を指示すると、記録されている伝言が、その人宛ての伝言である場合には、監視制御装置３は、記録されている伝言を、テレビ受像機７やスピーカ３５を通じて再生するようにするように構成されている。

【０１０９】

図１４は、この伝言記録および再生のための監視制御装置３の処理を説明するためのフローチャートである。この図１４の各ステップＳの処理は、ＣＰＵ２０１がＲＯＭ２０３に記憶されているプログラムにしたがって実行されるものである。

【０１１０】

すなわち、まず、使用者は、伝言記録または伝言再生をするには、自分の電子鍵装置４０を電子鍵リード／ライト部３６にかざして、通信を行なうようにする。ＣＰＵ２０１は、電子鍵リード／ライト部３６で電子鍵装置４０と通信が行なわれたか否か判別し（ステップＳ１）、通信が行われたと判別すると、受信した識別情報により、誰の電子鍵装置４０と通信したかを認識する（ステップＳ２）。

【０１１１】

次に、リモートコマンダ５０からのリモコン信号の到来を待ち（ステップＳ３）、リモコン信号を受信したことを確認したら、そのリモコン信号は、伝言記録ボタン５３の操作によるものか否か判別し（ステップＳ４）、伝言記録ボタン５３の操作によるものであると判別したときには、ＣＰＵ２０１は、伝言記録動作を行なうようにする（ステップＳ１２）。

【０１１２】

この伝言記録動作においては、監視制御装置３は、ビデオカメラ３１で撮影された伝言者の画像情報をカメラインターフェース２１０を介して取り込み、画像

・音声メモリ２０８の伝言記録領域に格納すると共に、マイクロホン３４で収音した伝言音声情報（伝言メッセージ）をインターフェース２１８を通じて取り込み、画像・音声メモリ２０８の伝言記録領域に格納する。このとき、それら画像情報および音声情報は、電子鍵装置４０から読み込んだ識別情報に対応付けられて、当該識別情報と共に画像・音声メモリ２０８に格納される。

【０１１３】

次に、ＣＰＵ２０１は、家族情報メモリ２０８に記憶されている家族の個人プロファイル情報を参照して、伝言記録をしようとしている操作者以外の伝言相手のリストをテレビ受像機７の画面に表示する（ステップＳ１４）。このとき、テレビ受像機７に電源が投入されていないときには、リモコン送信部３８を通じて電源をオンにするリモコン信号をテレビ受像機７に供給して、テレビ受像機７に電源を投入しておく。なお、伝言相手のリストの画面は、例えばスーパーインポーズによりテレビ番組の画像に重ねて表示するようにしてもよいし、テレビ番組の画像に重ねることなく単独の画面としてもよい。

【０１１４】

操作者は、この伝言相手のリストから、リモートコマンダ５０のカーソルキー５６を用いて、伝言相手の選択入力を行ない、カーソルキー５６中の中央の決定キーを押す。監視制御装置３のＣＰＵ２０１は、この伝言相手の選択入力を受信して（ステップＳ１５）、当該伝言相手の情報を、画像・音声メモリ２０８の伝言記録領域の、前記画像情報および伝言音声メッセージに対応させて格納して登録する（ステップＳ１６）。そして、伝言が記録されたことを報知するために、１個のＬＥＤ３７を点灯させる（ステップＳ１７）。ＬＥＤ３７は、図８に示したように複数個設けられており、記録されている伝言の数だけ、点灯することとなる。

【０１１５】

また、ステップＳ４において、リモコン信号が伝言記録ボタン５３の操作によるものではないと判別したときには、伝言再生ボタン５４の操作によるものであるか否か判別する（ステップＳ５）。伝言再生ボタン５４の操作によるものでないと判別したときには、ＣＰＵ２０１は、当該操作されたボタンに応じた処理を

行なう（ステップＳ６）。

【０１１６】

そして、ステップＳ５において、伝言再生ボタン５４の操作によるものであると判別したときには、ＣＰＵ２１は、ステップＳ２で認識した識別情報を検索子として、画像・音声メモリ２０８の伝言記録領域の記憶内容を検索して、電子鍵装置４０を電子鍵リード／ライト部３６にかざした操作者宛ての伝言があるか否か判別する（ステップＳ７）。

【０１１７】

そして、ステップＳ７において、操作者宛ての伝言が無いと判別したときには、ＣＰＵ２０１は、例えば予めＲＯＭ２０３に用意されている「伝言はありません」の文字情報をテレビ受像機７の画面に表示すると共に、スピーカ３５を通じて音声として放音して、操作者に報知する（ステップＳ８）。

【０１１８】

また、ステップＳ７において、操作者宛ての伝言が有ると判別したときには、当該操作者宛ての伝言画像および伝言音声を画像・音声メモリ２０８から読み出して、テレビ受像機７に表示すると共に、スピーカ３５から放音して再生する（ステップＳ９）。

【０１１９】

伝言の再生が終了すると、ＣＰＵ２０１は、テレビ受像機７の画面に伝言を消去するかどうかの問い合わせを表示するので、操作者は、その表示画面に含まれる「ＹＥＳ」、「ＮＯ」のいずれかをリモートコマンダ５０のカーソルキー５６を用いて選択する。ＣＰＵ２０１は、当該操作者の選択入力から、伝言を消去するか否か判別し（ステップＳ１０）、消去すると判別したときには、画像・音声メモリ２０８の対応する画像・音声情報を消去し（ステップＳ１１）、点灯しているＬＥＤ３７の一つを消灯する（ステップＳ１２）。そして、この伝言記録再生処理ルーチンを終了する。

【０１２０】

また、ステップＳ１０で、伝言を消去しないと判別したときには、そのまま、この伝言記録再生処理ルーチンを終了する。

【０１２１】

［ドアロック制御モードの選択設定；図１５、図１６］

前述したように、この実施形態では、監視制御装置３を通じてドアロック制御モードの設定ができるようにされているので、その設定動作を、図１５のフローチャートを参照しながら説明する。

【０１２２】

先ず、監視制御装置３のＣＰＵ２０１は、リモコン受信部３８の受信信号を監視して、ドアロック制御モードの設定を含む設定メニューのための特定のボタン操作がなされたか否か判別する（ステップＳ２１）。この例では、この特定のボタン操作としては、通常の使用者が行なわない操作とされており、例えばセキュリティボタン５１とメニューボタン５５との同時操作などとされている。このような特定のボタン操作は、ドアロック装置２の設置業者等が設定作業を行なうために定義されている。簡単に、ドアロック制御モードの設定変更ができないようにするためである。

【０１２３】

ステップＳ２１で、前記の特定のボタン操作はされないと判別されたときには、単独のボタン操作に応じた処理などの、その他の処理を行なう（ステップＳ２２）。また、ステップＳ２１で、前記の特定のボタン操作がされたと判別されたときには、設定メニューの一覧をテレビ受像機７の画面に、前述の伝言記録再生の場合と同様にして表示するようにする（ステップＳ２３）。

【０１２４】

この設定メニューの一覧表示に対しては、操作者は、行ないたい設定メニュー項目の選択をリモートコマンダ５０のカーソルキーを用いて行なう。ＣＰＵ２０１は、リモコン受信部３８の受信信号を監視してメニュー項目の選択操作がなされたか否か判別し（ステップＳ２４）、メニュー項目の選択操作がなされたと判別したときには、例えば反転表示して示す選択中項目を、選択操作に応じて変更する（ステップＳ２５）。そして、設定項目の決定操作がなされたか否か判別する（ステップＳ２６）。また、ステップＳ２４で、メニュー項目の選択操作がなされないと判別したときには、即座にステップＳ２６に進んで設定項目の決定操

作がなされたか否か判別する。

【０１２５】

ステップＳ２６で、設定項目の決定操作がなされないと判別したときには、ステップＳ２４に戻る。また、ステップＳ２６で、設定項目の決定操作がなされたと判別したときには、選択された設定項目はドアロック制御モードの設定であるか否か判別し（ステップＳ２７）、そうではなかったときには選択された他の設定項目についての処理ルーチンを実行する（ステップＳ２８）。

【０１２６】

ステップＳ２７で、選択された設定項目はドアロック制御モードの設定であると判別したときには、ＣＰＵ２０１は、テレビ受像機７の画面にオートロックモードと、逐次ロックモードとの選択画面を表示する（ステップＳ２９）。操作者は、この選択画面において、いずれかの選択入力をカーソルキー５６を用いて行なう。

【０１２７】

そこで、ＣＰＵ２０１は、リモコン受信部３８を監視して、オートロックモードが選択されたか否か判別し（ステップＳ３０）、オートロックモードが選択されたと判別したときには、ドアロック装置２をオートロックモードに設定する設定動作を行なう（ステップＳ３１）。

【０１２８】

すなわち、ＣＰＵ２０１は、監視制御装置３に内蔵の不揮発性メモリ部のドアロック装置２のドアロック制御モードの記憶領域に、オートロックモードであることを示す情報を記憶すると共に、オートロックモードにする旨の指示をドアロック装置２に対して、ドアロック装置通信インターフェース２０６を通じて送る。

【０１２９】

また、ステップＳ３０で、オートロックモードではないと判別したときには、ＣＰＵ２０１は、逐次ロックモードが選択されたと判別して、ドアロック装置２を逐次ロックモードにする設定動作を行なう（ステップＳ３２）。

【０１３０】

すなわち、ＣＰＵ２０１は、監視制御装置３に内蔵の不揮発性メモリ部のドアロック装置２のドアロック制御モードの記憶領域に、逐次ロックモードであることを示す情報を記憶すると共に、逐次ロックモードにする旨の指示をドアロック装置２に対して、ドアロック装置通信インターフェース２０６を通じて送る。

【０１３１】

以上で、監視制御装置３におけるロック制御モードの設定時の動作は終了となる。

【０１３２】

次に、ドアロック装置通信インターフェース２０６を通じて送られてきたドアロック制御モードの指示情報を受信したドアロック制御装置１００の動作について、図１１のフローチャートを参照して説明する。

【０１３３】

先ず、ドアロック制御装置１００のＣＰＵ１０１は、ドアロック制御モードの設定指示情報を監視制御装置３から受け取ったか否か判別し（ステップＳ４１）、受け取らないときには、その他の処理を行なう（ステップＳ４２）。

【０１３４】

ステップＳ４１で、ドアロック制御モードの設定指示情報を監視制御装置３から受け取ったと判別したときには、ＣＰＵ１０１は、選択指示されたドアロック制御モードは、オートロックモードと逐次ロックモードのいずれであるか判別する（ステップＳ４３）。

【０１３５】

ステップＳ４３で、選択指示されたドアロック制御モードはオートロックモードであると判別したときには、ＣＰＵ１０１は、ドアロック装置２のドアロック制御モードをオートロックモードに設定する処理を行なう（ステップＳ４４）。

【０１３６】

すなわち、ステップＳ４４においては、ドアロック制御装置１００のＣＰＵ１０１は、オートロックモードの設定指示に基づき、ドアロック装置２の内側電子鍵リード／ライト部２１ｉｎと、外側電子鍵リード／ライト部２１ｅｘとの両方をアクティブにし、かつ、プログラムＲＯＭ１３のドアロック制御のアプリケー

ションを、オートロックモード用のものとするようにする。そして、ＣＰＵ１０１は、ドアロック制御装置１００が備える不揮発性メモリ部のドアロック制御モードの記憶領域に、オートロックモードであることを示す情報を記憶する。

【０１３７】

また、ステップＳ４３で、選択指示されたドアロック制御モードは逐次ロックモードであると判別したときには、ＣＰＵ１０１は、ドアロック装置２のドアロック制御モードを逐次ロックモードに設定する処理を行なう（ステップＳ４５）。

【０１３８】

すなわち、ステップＳ４５においては、ドアロック制御装置１００のＣＰＵ１０１は、逐次ロックモードの設定指示に基づき、この例では、ドアロック装置２の内側電子鍵リード／ライト部２１ｉｎと、外側電子鍵リード／ライト部２１ｅｘとの両方をアクティブにし、かつ、プログラムＲＯＭ１３のドアロック制御のアプリケーションを、逐次ロックモード用のものとするようにする。そして、ＣＰＵ１０１は、ドアロック制御装置１００が備える不揮発性メモリ部のドアロック制御モードの記憶領域に、逐次ロックモードであることを示す情報を記憶する。

【０１３９】

なお、この例では、逐次ロックモードにおいても、内側電子鍵リード／ライト部２１ｉｎと、外側電子鍵リード／ライト部２１ｅｘとの両方を用いるようにしたが、この逐次ロックモードにおいては、外側電子鍵リード／ライト部ｅｘのみをアクティブにして、内側電子鍵リード／ライト部２１ｉｎを用いないようにすることもできる。その場合には、家の内側からの施錠が問題になるが、例えば、内側からの玄関ドアの施錠を、電子鍵装置を用いずにマニュアル操作で行なえる構成とすればよい。

【０１４０】

次に、オートロックモードと、逐次ロックモードのそれぞれの場合のドアロック装置２の動作について説明する。以下に説明するフローチャートにおける各ステップＳの動作は、ドアロック制御装置１００のＣＰＵ１０１が主として実行す

る処理動作である。

【０１４１】

［オートロックモード；図１７～図２２］

オートロックモードのときの動作を、図１７～図２２のフローチャートを参照しながら説明する。このオートロックモードのときには、玄関ドア１は、定常状態では、施錠状態とされる。そして、電子鍵装置４０が、内側電子鍵リード／ライト部２１ｉｎまたは外側電子鍵リード／ライト部２１ｅｘにかざされて通信が両者の間で行なわれ、識別情報、すなわち、電子鍵情報についての認証がとれたときには、所定時間のみ玄関ドアを開錠し、所定時間後に、自動的に玄関ドア１は施錠状態に戻るように、ドアロック制御装置１００により制御されるものである。

【０１４２】

ＣＰＵ１０１は、インターフェース１０５，１０６を介して、内側電子鍵リード／ライト部２１ｉｎおよび外側電子鍵リード／ライト部２１ｅｘを監視し、電子鍵装置４０がかざされて、電子鍵装置４０と内側電子鍵リード／ライト部２１ｉｎまたは外側電子鍵リード／ライト部２１ｅｘとの間で通信が行われるのを待つ（ステップＳ５１）。

【０１４３】

そして、ステップＳ５１において、電子鍵装置４０がかざされて、電子鍵装置４０と通信が行なわれたと判別したときには、ＣＰＵ１０１は、識別情報を電子鍵装置４０から受信し、例えばＲＡＭ１０４などに一時的に格納する（ステップＳ５２）。このとき、ドアロック制御装置１００が備える時計回路（図示を省略）の時刻情報が、電子鍵装置４０に与えられ、制御用ＩＣ内４２のメモリに書き込まれる。また、内側電子鍵リード／ライト部２１ｉｎまたは外側電子鍵リード／ライト部２１ｅｘのどちらと通信をしたかの情報として、通信相手のＩＤ等が制御用ＩＣ４２のメモリに書き込まれる。

【０１４４】

次に、ＣＰＵ１０１は、内側電子鍵リード／ライト部２１ｉｎまたは外側電子鍵リード／ライト部２１ｅｘのどちらで電子鍵装置４０と通信が行われたかを判

別する（ステップＳ５３）。その判別結果と、前記の通信の時刻情報とは、家族情報メモリ１２０の、前記識別情報に対応する家人の記録エリアにも書き込まれ、また、監視制御装置３にも、その家族情報メモリ２０５に記憶させるために転送される。

【０１４５】

[内側電子鍵リード／ライト部２１ｉｎでの通信の場合；図１７～図１９]

ステップＳ５３で、電子鍵装置４０と通信が行われたのが内側電子鍵リード／ライト部２１ｉｎであると判別したときには、ＣＰＵ１０１は、在宅者が外出する場合であるとして、以下のような処理を行なう。なお、この例では、在宅者が玄関ドア１を開錠し、玄関ドア１を開けたときには、それまでにセキュリティモードがオンになっていても、一旦、セキュリティモードは、オフとされるものとしている。

【０１４６】

ＣＰＵ１０１は、先ず、家族情報メモリ１２０に記憶されている識別情報と、電子鍵装置４０から受信した識別情報とを比較して、家族情報メモリ１２０に記憶されている電子鍵情報としての識別情報の中に、電子鍵装置４０から受信した識別情報と一致するものがあるかどうかにより、当該電子鍵装置４０がドアロック装置２に登録された電子鍵装置であるか否かを判別して、当該電子鍵装置４０についての認証を行なう（ステップＳ５４）。

【０１４７】

そして、その認証結果を判別し（ステップＳ５５）、家族情報メモリ１２０に記憶されている識別情報の中に、電子鍵装置４０から受信した識別情報と一致するものがなくて、認証が取れなかったとき（認証ＮＧ）であると判別したときには、ＣＰＵ１０１は、内側ＬＥＤ駆動部１０７を駆動して、内側ＬＥＤ２２ｉｎを赤色で点滅させると共に、内側スピーカ２３ｉｎから警告音を放音して、認証ＮＧであることを電子鍵装置４０の使用者に報知する（ステップＳ５６）。そして、ドアロック機構２８は施錠状態のままとして、ステップＳ５１に戻る。

【０１４８】

また、ステップＳ５５で、家族情報メモリ１２０に記憶されている識別情報の

中に、電子鍵装置４０から受信した識別情報と一致するものがあって、認証がＯＫであると判別したときには、ＣＰＵ１０１は、内側ＬＥＤ駆動部１０７を駆動して、内側ＬＥＤ２２ｉｎを緑色で１秒間点灯させ、認証ＯＫであることを電子鍵装置４０の使用者に報知する（ステップＳ５７）。このとき、ＣＰＵ１０１により、併せて内側スピーカ２３ｉｎから「認証がとれました」というメッセージを放音させるようにしても良い。

【０１４９】

そして、このとき、認証がＯＫであることから、ＣＰＵ１０１は、ドアロック機構駆動部１１２を駆動制御して、ドアロック機構２８により玄関ドア１を開錠状態にし（ステップＳ５８）、内側スピーカ２３ｉｎから、「ドアロックを解除しました」というメッセージを放音させる（ステップＳ５９）。このとき、内側ＬＥＤ２２ｉｎを、例えば緑色で点滅させ、ドアロックの解除状態を電子鍵装置４０の使用者に報知するようにしてもよい。

【０１５０】

このとき、ＣＰＵ１０１は、電子鍵装置４０により内側から玄関ドア１が開錠されたことを認識していることに基づき、当該電子鍵装置４０の使用者（在宅者）が外出しようとしていると認識する。そして、監視制御装置３に対して窓の開閉状態についての問い合わせを送る（図１３のステップＳ６１）。

【０１５１】

これに対して、監視制御装置３では、窓センサ６ａ，６ｂのセンサ出力をセンサハブ２０７を通じて取得して、窓の開閉を確認する。つまり、戸締りを確認する。そして、窓の開閉状態についての確認結果をドアロック装置インターフェース２０６を通じてドアロック制御装置１００に返信するようにする。

【０１５２】

ドアロック制御装置１００では、この窓の開閉状態についての確認結果を、通信インターフェース１２１を通じて受信する（ステップＳ６２）。そして、ＣＰＵ１０１は、受信した当該確認結果を解析して、窓が開放されているか否か判別する（ステップＳ６３）。

【０１５３】

そして、窓が開いていると判別したときには、ＣＰＵ１０１は、窓が開いていることを内側スピーカ２３ｉｎからの放音音声により警告する（ステップＳ６４）。また、窓が閉じていると判別したときには、ＣＰＵ１０１は、戸締りがＯＫであることを内側スピーカ２３ｉｎからの放音音声により報知する（ステップＳ６５）。

【０１５４】

次に、ＣＰＵ１０１は、ドア開閉センサ２７のセンサ出力をインターフェース１１１を通じて取り込み、玄関ドア１が開けられた否か監視する（ステップＳ６６）。そして、ＣＰＵ１０１は、玄関ドア１が開けられずに所定時間、例えば１０秒経過したかどうかを判別し（ステップＳ６７）、１０秒経過したと判別したときには、玄関ドア１を自動的に施錠状態に戻すようにする（ステップＳ６８）。そして、ＣＰＵ１０１は、内側ＬＥＤ２２ｉｎを緑色で点滅して、玄関ドア１が施錠状態に戻ったことを報知する（ステップＳ６９）。

【０１５５】

また、ステップＳ６６で、ステップＳ５８での開錠後、１０秒以内に玄関ドア１が開かれたと判別したときには、ＣＰＵ１０１は、ステップＳ５２で取り込んだ識別情報で示される在宅者が外出をしたと認識して、当該識別情報を含む個人情報を、外出者情報として監視制御装置３に転送する（ステップＳ７０）。

【０１５６】

その後、ＣＰＵ１０１は、ドア開閉センサ２７のセンサ出力を参照して、玄関ドア１が閉じられたことを確認し（ステップＳ７１）、玄関ドア１が閉じられた後、所定時間、例えば３秒経過したことを確認したら（ステップＳ７２）、ドアロック機構駆動部１１２を駆動制御して、ドアロック機構２８により玄関ドア１を施錠状態に復帰させるようにする（図１９のステップＳ８１）。そして、ＣＰＵ１０１は、外側ＬＥＤ２２ｅｘを緑色で点滅して、玄関ドア１が施錠状態に戻ったことを電子鍵装置４０の使用者に報知する（ステップＳ８２）。この外側ＬＥＤ２２ｅｘの緑色点滅は、所定時間、例えば１０秒間続けられる。

【０１５７】

その後、ＣＰＵ１０１は、前記所定時間、例えば１０秒経過したか否か判別し

（ステップＳ８３）、所定時間経過していないと判別したときには、ステップＳ５１で通信が行われたと判別された電子鍵装置が、再度、外側電子鍵リード／ライト部２１ｅｘと通信したか否か判別する（ステップＳ８４）、通信がなされないと判別したときにはステップＳ８３に戻る。

【０１５８】

そして、ステップＳ８３で、電子鍵装置と外側電子鍵リード／ライト部２１ｅｘとで通信が行われずに、前記所定時間経過したと判別したときには、ＣＰＵ１０１は、内側電子鍵リード／ライト部２１ｉｎに対して電子鍵装置がかざされたことにより開始された玄関ドアのロック制御動作が一段落したとして、図１７のステップＳ５１に戻る。

【０１５９】

また、ステップＳ８４で、玄関ドア施錠復帰後、外側ＬＥＤ２２ｅｘの緑色点滅が終了する所定時間経過する前に、ステップＳ５１において通信が行われたと判別された電子鍵装置と外側電子鍵リード／ライト部２１ｅｘとで通信が行われたと判別すると、ステップＳ６１～Ｓ６３で確認された戸締りを再確認する（ステップＳ８５）。

【０１６０】

ステップＳ８５で、戸締りがＯＫであると判別したときには、ＣＰＵ１０１は、通信インターフェース１２１を通じてセキュリティモードをオンにする要求を監視制御装置３に送信する（ステップＳ８６）。

【０１６１】

この要求に対しては、監視制御装置３は、そのときの在宅状況をチェックして、セキュリティレベルが図１１に示したいずれのレベルとなるかを判定する。そして、監視制御装置３は、その判定の結果、セキュリティレベルがレベルＤであるときには、セキュリティモードはオンにできないので、その旨をドアロック制御装置１００に返し、セキュリティレベルがレベルＤ以外であるときには、セキュリティモードをオンにできるので、その旨をドアロック制御装置１００に返す。

【０１６２】

ドアロック制御装置１００のＣＰＵ１０１は、監視制御装置３からのセキュリティモードオンの要求に対する返答を解析して、セキュリティモードをオンにできるか否か判別する（ステップＳ８７）。そして、セキュリティモードがオンにできる旨の返答を監視制御装置３から受けたと判別したときには、ＣＰＵ１０１は、外側スピーカ２３ｅｘから、「セキュリティモードをオンにします」というメッセージを放音させる（ステップＳ８８）。

【０１６３】

また、ステップＳ８７で、セキュリティモードがオンにできない旨の返答を監視制御装置３から受けたと判別したときには、ＣＰＵ１０１は、外側スピーカ２３ｅｘから、「在宅者が存在するため、セキュリティモードをオンにはできません」というメッセージを放音させる（ステップＳ８９）。その後、ステップＳ５１に戻る。

【０１６４】

また、ステップＳ８５で、窓が開いていて戸締りが完了していないと判別したときには、ＣＰＵ１０１は、「窓が開いているため、セキュリティモードをオンにすることはできません」という警告メッセージを放音する（ステップＳ９０）。そして、その後、ステップＳ５１に戻る。

【０１６５】

[外側電子鍵リード／ライト部２１ｅｘでの通信の場合；図２０～図２２]

ステップＳ５１で、電子鍵装置４０と通信が行われたのが外側電子鍵リード／ライト部２１ｅｘであると判別したときには、ＣＰＵ１０１は、家人が帰宅した場合あるいはその他の外にいる者の入室要求であるとして、以下のような処理を行なう。

【０１６６】

ＣＰＵ１０１は、まず、家族情報メモリ１２０に記憶されている識別情報と、電子鍵装置４０から受信した識別情報とを比較して、家族情報メモリ１２０に記憶されている識別情報の中に、電子鍵装置４０から受信した識別情報と一致するものがあるかどうかにより、当該電子鍵装置４０がドアロック装置２に登録された電子鍵装置であるか否かを判別して、当該電子鍵装置４０についての認証を行

なう（ステップＳ１０１）。

【０１６７】

そして、その認証結果を判別し（ステップＳ１０２）、家族情報メモリ１２０に記憶されている識別情報の中に、電子鍵装置４０から受信した識別情報と一致するものがなくて、認証が取れなかったとき（認証ＮＧ）であると判別したときには、ＣＰＵ１０１は、外側ＬＥＤ駆動部１０８を駆動して、外側ＬＥＤ２２ｅｘを赤色で点滅させると共に、外側スピーカ２３ｅｘから警告音を放音して、認証ＮＧであることを電子鍵装置４０の使用者に報知する（ステップＳ１０３）。そして、ドアロック機構２８は施錠状態のままとして、ステップＳ５１に戻る。

【０１６８】

また、ステップＳ１０２で、家族情報メモリ１２０に記憶されている識別情報の中に、電子鍵装置４０から受信した識別情報と一致するものがあって、認証がＯＫであると判別したときには、ＣＰＵ１０１は、外側ＬＥＤ駆動部１０８を駆動して、外側ＬＥＤ２２ｅｘを緑色で１秒間点灯させ、認証ＯＫであることを電子鍵装置４０の使用者に報知する（ステップＳ１０４）。このとき、ＣＰＵ１０１により、合わせて外側スピーカ２３ｅｘから「認証がとれました」というメッセージを放音させるようにしても良い。

【０１６９】

そして、このとき、認証がＯＫであることから、ＣＰＵ１０１は、ドアロック機構駆動部１１２を駆動制御して、ドアロック機構２８により玄関ドア１を開錠状態にし（ステップＳ１０５）、外側スピーカ２３ｅｘから、「ドアロックを解除しました」というメッセージを放音させる（ステップＳ１０６）。このとき、外側ＬＥＤ２２ｅｘを、例えば緑色で点滅させ、ドアロックの解除状態を電子鍵装置４０の使用者に報知するようにしてもよい。

【０１７０】

次に、ＣＰＵ１０１は、ドア開閉センサ２７のセンサ出力をインターフェース１１１を通じて取り込み、玄関ドア１が開けられた否か監視する（ステップＳ１０７）。そして、ＣＰＵ１０１は、玄関ドア１が開けられずに所定時間、例えば１０秒経過したかどうかを判別し（ステップＳ１０８）、１０秒経過したと判別

したときには、玄関ドア１を自動的に施錠状態に戻すようにする（ステップＳ１０９）。そして、ＣＰＵ１０１は、外側ＬＥＤ２２ｅｘを緑色で点滅して、玄関ドア１が施錠状態に戻ったことを報知する（ステップＳ１１０）。

【０１７１】

その後、ＣＰＵ１０１は、所定時間、例えば１０秒経過したか否か判別し（ステップＳ１１１）、所定時間経過していないと判別したときには、ステップＳ５１で通信が行われたと判別された電子鍵装置が外側電子鍵リード／ライト部２１ｅｘと通信したか否か判別し（ステップＳ１１２）、通信がなされないと判別したときにはステップＳ１１１に戻る。

【０１７２】

そして、ステップＳ１１１で、電子鍵装置と外側電子鍵リード／ライト部２１ｅｘとで通信が行われずに、所定時間経過したと判別したときには、ＣＰＵ１０１は、外側電子鍵リード／ライト部２１ｅｘに対して電子鍵装置がかざされたことにより開始された玄関ドアのロック制御動作が一段落したとして、図１７のステップＳ５１に戻る。

【０１７３】

また、ステップＳ１１２で、玄関ドア施錠復帰後、所定時間経過する前に、ステップＳ５１において通信が行われたと判別された電子鍵装置と外側電子鍵リード／ライト部２１ｅｘとで通信が行われたと判別すると、戸締りを確認する（ステップＳ１１３）。

【０１７４】

このステップＳ１１３での戸締りの確認は、前述のステップＳ６１～Ｓ６３において説明した処理と同様に行なう。つまり、ドアロック制御装置１００は、監視制御装置３に対して窓の開閉状態についての問い合わせを行ない、問い合わせ結果を監視制御装置３から取得する。そして、その問い合わせ結果から、戸締りがＯＫかどうかを判別する。

【０１７５】

ステップＳ１１３で、戸締りがＯＫであると判別したときには、ＣＰＵ１０１は、通信インターフェース１２１を通じてセキュリティモードをオンにする要求

を監視制御装置３に送信する（ステップＳ１１４）。

【０１７６】

この要求に対しては、監視制御装置３は、そのときの在宅状況をチェックして、セキュリティレベルが図１１に示したいずれのレベルとなるかを判定する。そして、監視制御装置３は、その判定の結果、セキュリティレベルがレベルＤであるときには、セキュリティモードはオンにできないので、その旨をドアロック制御装置１００に返し、セキュリティレベルがレベルＤ以外であるときには、セキュリティモードをオンにできるので、その旨をドアロック制御装置１００に返す。

【０１７７】

ドアロック制御装置１００のＣＰＵ１０１は、監視制御装置３からのセキュリティモードオンの要求に対する返答を解析して、セキュリティモードをオンにできるか否か判別する（ステップＳ１１５）。そして、セキュリティモードがオンにできる旨の返答を監視制御装置３から受けたと判別したときには、ＣＰＵ１０１は、外側スピーカ２３ｅｘから、「セキュリティモードをオンにします」というメッセージを放音させる（ステップＳ１１６）。

【０１７８】

また、ステップＳ１１５で、セキュリティモードがオンにできない旨の返答を監視制御装置３から受けたと判別したときには、ＣＰＵ１０１は、外側スピーカ２３ｅｘから、「在宅者が存在するため、セキュリティモードをオンにはできません」というメッセージを放音させる（ステップＳ１１７）。その後、ステップＳ５１に戻る。

【０１７９】

また、ステップＳ１１３で、窓が開いていて戸締りが完了していないと判別したときには、ＣＰＵ１０１は、「窓が開いているため、セキュリティモードをオンにすることはできません」という警告メッセージを放音する（ステップＳ１１８）。そして、その後、ステップＳ５１に戻る。

【０１８０】

ステップＳ１１１～ステップＳ１１８の処理は、一旦、玄関ドア１を内側から

開錠した後、所定時間以内に、外側電子鍵リード／ライト部２１ｅｘに電子鍵装置をかざして、セキュリティモードをオンにするのを忘れた者が、もう一度、室内に戻って、内側電子鍵リード／ライト部２１ｉｎに対して電子鍵装置をかざすところからやり直す手間を防止するための処理である。

【０１８１】

すなわち、一旦、玄関ドア１を内側から開錠した後、所定時間以内に、外側電子鍵リード／ライト部２１ｅｘに電子鍵装置をかざして、セキュリティモードをオンにするのを忘れた、あるいは失敗した場合に、外側電子鍵リード／ライト部２１ｅｘに電子鍵装置をかざして、玄関ドア１を一旦開錠させ、その後、１０秒待って再施錠になった後、１０秒以内に、再び、外側電子鍵リード／ライト部２１ｅｘに電子鍵装置をかざすことにより、セキュリティモードをオンにすることができるものである。このようにすれば、セキュリティモードをオンに設定するために、開錠してから室内に入り、内側電子鍵リード／ライト部２１ｉｎに電子鍵装置４０をかざすところからやり直す必要がなく、便利である。

【０１８２】

次に、ステップＳ１０７で、ステップＳ１０５での開錠後、１０秒以内に玄関ドア１が開かれたと判別したときには、ＣＰＵ１０１は、ステップＳ５２で取り込んだ識別情報で示される外出者が帰宅したと認識して、当該識別情報を含む個人情報を、帰宅者情報として監視制御装置３に転送する（図２２のステップＳ１２１）。

【０１８３】

その後、ＣＰＵ１０１は、ドア開閉センサ２７のセンサ出力を参照して、玄関ドア１が閉じられたことを確認し（ステップＳ１２２）、玄関ドア１が閉じられた後、所定時間、例えば３秒経過したことを確認したら（ステップＳ１２３）、ドアロック機構駆動部１１２を駆動制御して、ドアロック機構２８により玄関ドア１を施錠状態に復帰させるようにする（ステップＳ１２４）。そして、ＣＰＵ１０１は、内側ＬＥＤ２２ｉｎを緑色で点滅して、玄関ドア１が施錠状態に戻ったことを報知する（ステップＳ１２５）。

【０１８４】

その後、ＣＰＵ１０１は、帰宅者があったことから在宅状況が変更することに基づき、セキュリティレベルの変更指示を監視制御装置３に送る（ステップＳ１２６）。

【０１８５】

このセキュリティレベルの変更指示を受け取った監視制御装置３では、ステップＳ１２１での帰宅者情報による在宅状況の変化を認識し、図１１に示した在宅状況とセキュリティレベルとの対応テーブルを参照して、セキュリティレベルの変更の必要があるか否か判別し、必要があるときには、セキュリティレベルを変更する。そして、監視制御装置３は、セキュリティレベルを変更したかどうかを、ドアロック制御装置１００に通知する。

【０１８６】

ドアロック制御装置１００のＣＰＵ１０１は、監視制御装置３からのセキュリティレベルの変更に関する通知を受け取って（ステップＳ１２７）、セキュリティレベルが変更されたか否かを判別する（ステップＳ１２８）。

【０１８７】

そして、ステップＳ１２８で、セキュリティモードが変更されたと判別したときには、ＣＰＵ１０１は、内側スピーカ２３ｉｎから、「セキュリティレベルを変更しました」というメッセージを放音する（ステップＳ１２９）。そして、ステップＳ５１に戻る。

【０１８８】

なお、以上の説明では、帰宅者があったときには、ドアロック制御装置１００から、ステップＳ１２６において、監視制御装置３にセキュリティレベルの変更指示を送るようにしたが、監視制御装置３では、ステップＳ１２１での帰宅者情報の転送を受けるので、ドアロック制御装置１００からのセキュリティレベルの変更指示を受けなくても、自動的にセキュリティレベルの変更が必要かどうかを判断して、必要である場合には、セキュリティレベルを自動的に変更するようにしても良い。その場合には、セキュリティレベルを変更したときには、その旨をドアロック制御装置１００に転送するようにする。

【０１８９】

［逐次ロックモードの説明；図２３～図２５］

次に、逐次ロックモードのときの動作を、図２３～図２５のフローチャートを参照しながら説明する。この逐次ロックモードのときには、電子鍵装置４０が、内側電子鍵リード／ライト部２１ｉｎまたは外側電子鍵リード／ライト部２１ｅｘにかざされて通信が両者の間で行なわれ、電子鍵情報としての識別情報についての認証がとれたときには、そのときの玄関ドア１の開錠あるいは施錠の状態とは逆の状態になるように、ドアロック機構２８は、ドアロック制御装置１００により制御されるものである。

【０１９０】

ＣＰＵ１０１は、インターフェース１０５，１０６を介して、内側電子鍵リード／ライト部２１ｉｎおよび外側電子鍵リード／ライト部２１ｅｘを監視し、電子鍵装置４０がかざされて、電子鍵装置４０と内側電子鍵リード／ライト部２１ｉｎまたは外側電子鍵リード／ライト部２１ｅｘとの間で通信が行われるのを待つ（ステップＳ１３１）。

【０１９１】

そして、ステップＳ１３１において、電子鍵装置４０がかざされて、電子鍵装置４０と通信が行なわれたと判別したときには、ＣＰＵ１０１は、識別情報を電子鍵装置４０から受信し、例えばＲＡＭ１０４などに一時的に格納する（ステップＳ１３２）。このとき、前述と同様に、電子鍵装置４０には時刻情報等が書き込まれると共に、家族情報メモリ１２０および監視制御装置３の家族情報メモリ２０５への時刻情報等の書き込みが行なわれる。

【０１９２】

内側電子鍵リード／ライト部２１ｉｎまたは外側電子鍵リード／ライト部２１ｅｘのどちらで電子鍵装置４０と通信が行われたかを判別する（ステップＳ１３３）。

【０１９３】

［内側電子鍵リード／ライト部２１ｉｎでの通信の場合；図２３］

ステップＳ１３３で、電子鍵装置４０と通信が行われたのが内側電子鍵リード／ライト部２１ｉｎであると判別したときには、ＣＰＵ１０１は、在宅者が外出

する場合あるいは玄関ドア１をセキュリティのために施錠する場合であるとして、以下のような処理を行なう。

【０１９４】

ＣＰＵ１０１は、先ず、家族情報メモリ１２０に記憶されている識別情報と、電子鍵装置４０から受信した識別情報とを比較して、家族情報メモリ１２０に記憶されている識別情報の中に、電子鍵装置４０から受信した識別情報と一致するものがあるかどうかにより、当該電子鍵装置４０がドアロック装置２に登録された電子鍵装置であるか否かを判別して、当該電子鍵装置４０についての認証を行なう（ステップＳ１３４）。

【０１９５】

そして、その認証結果を判別し（ステップＳ１３５）、家族情報メモリ１２０に記憶されている識別情報の中に、電子鍵装置４０から受信した識別情報と一致するものがなくて、認証が取れなかったとき（認証ＮＧ）であると判別したときには、ＣＰＵ１０１は、内側ＬＥＤ駆動部１０７を駆動して、内側ＬＥＤ２２ｉｎを赤色で点滅させると共に、内側スピーカ２３ｉｎから警告音を放音して、認証ＮＧであることを電子鍵装置４０の使用者に報知する（ステップＳ１３６）。そして、ドアロック機構２８は、その前の状態のままとして、ステップＳ１３１に戻る。

【０１９６】

また、ステップＳ１３５で、家族情報メモリ１２０に記憶されている識別情報の中に、電子鍵装置４０から受信した識別情報と一致するものがあって、認証がＯＫであると判別したときには、ＣＰＵ１０１は、内側ＬＥＤ駆動部１０７を駆動して、内側ＬＥＤ２２ｉｎを緑色で１秒間点灯させ、認証ＯＫであることを電子鍵装置４０の使用者に報知する（ステップＳ１３７）。このとき、ＣＰＵ１０１により、併せて内側スピーカ２３ｉｎから「認証がとれました」というメッセージを放音させるようにしても良い。

【０１９７】

そして、ＣＰＵ１０１は、現在のドアロック機構２８による玄関ドア１のロック状態は、施錠状態になっているか否か判別する（ステップＳ１３８）。このス

テップＳ１３８で、ドアロック機構２８による玄関ドア１のロック状態が、開錠状態であると判別したときには、その逆の状態である施錠状態にするように、ドアロック機構駆動部１１２を駆動制御する（ステップＳ１３９）。

【０１９８】

そして、ＣＰＵ１０１は、内側ＬＥＤ２２ｉｎを、例えば緑色で点滅させると共に、内側スピーカ２３ｉｎから、「玄関ドアを施錠しました」というメッセージを放音させ、施錠状態にしたことを電子鍵装置４０の使用者に報知するようにする（ステップＳ１４０）。

【０１９９】

そして、ＣＰＵ１０１は、ステップＳ１３２で取り込んだ識別情報で示される者が、セキュリティのために施錠をしたと認識して、当該識別情報を含む個人情報を、在宅者情報として監視制御装置３に転送する（ステップＳ１４１）。

【０２００】

また、ステップＳ１３８で、現在のドアロック機構２８のロック状態は、施錠状態であると判別したときには、ＣＰＵ１０１は、ドアロック機構駆動部１１２を駆動制御して、ドアロック機構２８を開錠状態にし（ステップＳ１４２）、内側ＬＥＤ２２ｉｎを、例えば緑色で点滅させると共に、内側スピーカ２３ｉｎから、「ドアロックを解除しました」というメッセージを放音させる（ステップＳ１４３）。

【０２０１】

そして、このときには、ＣＰＵ１０１は、ステップＳ１３２で取り込んだ識別情報で示される者が、開錠をして外出をしたと認識して、当該識別情報を含む個人情報を、外出者情報として監視制御装置３に転送する（ステップＳ１４４）。

【０２０２】

［外側電子鍵リード／ライト部２１ｅｘでの通信の場合；図２４～図２５］

ステップＳ１３３で、電子鍵装置４０と通信が行われたのが外側電子鍵リード／ライト部２１ｅｘであると判別したときには、ＣＰＵ１０１は、家人が帰宅して開錠する場合あるいは家人が外出のため施錠する場合であるとして、以下のような処理を行なう。

【０２０３】

ＣＰＵ１０１は、まず、家族情報メモリ１２０に記憶されている識別情報と、電子鍵装置４０から受信した識別情報とを比較して、家族情報メモリ１２０に記憶されている識別情報の中に、電子鍵装置４０から受信した識別情報と一致するものがあるかどうかにより、当該電子鍵装置４０がドアロック装置２に登録された電子鍵装置であるか否かを判別して、当該電子鍵装置４０についての認証を行なう（ステップＳ１５１）。

【０２０４】

そして、その認証結果を判別し（ステップＳ１５２）、家族情報メモリ１２０に記憶されている識別情報の中に、電子鍵装置４０から受信した識別情報と一致するものがなくて、認証が取れなかったとき（認証ＮＧ）であると判別したときには、ＣＰＵ１０１は、外側ＬＥＤ駆動部１０８を駆動して、外側ＬＥＤ２２ｅｘを赤色で点滅させると共に、外側スピーカ２３ｅｘから警告音を放音して、認証ＮＧであることを電子鍵装置４０の使用者に報知する（ステップＳ１５３）。そして、ドアロック機構２８は施錠状態のままとして、ステップＳ１３１に戻る。

【０２０５】

また、ステップＳ１０２で、家族情報メモリ１２０に記憶されている識別情報の中に、電子鍵装置４０から受信した識別情報と一致するものがあって、認証がＯＫであると判別したときには、ＣＰＵ１０１は、外側ＬＥＤ駆動部１０８を駆動して、外側ＬＥＤ２２ｅｘを緑色で１秒間点灯させ、認証ＯＫであることを電子鍵装置４０の使用者に報知する（ステップＳ１５４）。このとき、ＣＰＵ１０１により、併せて外側スピーカ２３ｅｘから「認証がとれました」というメッセージを放音させるようにしても良い。

【０２０６】

そして、ＣＰＵ１０１は、現在のドアロック機構２８のロック状態は、施錠状態になっているか否か判別する（ステップＳ１５５）。このステップＳ１５５で、現在のドアロック機構２８による玄関ドア１のロック状態は、施錠状態であると判別したときには、ＣＰＵ１０１は、ドアロック機構駆動部１１２を駆動制御

して、ドアロック機構２８により玄関ドア１を開錠状態にし（ステップＳ１５６）、内側ＬＥＤ２２ｉｎを、例えば緑色で点滅させると共に、内側スピーカ２３ｉｎから、「ドアロックを解除しました」というメッセージを放音させる（ステップＳ１５７）。

【０２０７】

そして、ＣＰＵ１０１は、ステップＳ１３２で取り込んだ識別情報で示される者が、帰宅のため開錠をしたと認識して、当該識別情報を含む個人情報を、帰宅者情報として監視制御装置３に転送する（ステップＳ１５８）。

【０２０８】

また、ステップＳ１５５で、現在の玄関ドア１のロック状態が開錠状態であると判別したときには、その逆の状態である施錠状態にするように、ドアロック機構駆動部１１２を駆動制御して、ドアロック機構２８により玄関ドア１を施錠状態にする（ステップＳ１５９）。

【０２０９】

そして、ＣＰＵ１０１は、内側ＬＥＤ２２ｉｎを、例えば緑色で点滅させると共に、内側スピーカ２３ｉｎから、「玄関ドアを施錠しました」というメッセージを放音させ、施錠状態にしたことを電子鍵装置４０の使用者に報知するようにする（ステップＳ１６０）。

【０２１０】

そして、ＣＰＵ１０１は、ステップＳ１３２で取り込んだ識別情報で示される者が、外出のために施錠をしたと認識して、当該識別情報を含む個人情報を、外出者情報として監視制御装置３に転送する（ステップＳ１６１）。

【０２１１】

そして、施錠後、ＣＰＵ１０１は、所定時間、例えば１０秒経過したか否か判別し（図２５のステップＳ１６２）、所定時間経過していないと判別したときには、ステップＳ１３１で通信が行われたと判別された電子鍵装置が、再度、外側電子鍵リード／ライト部２１ｅｘと通信したか否か判別し（ステップＳ１６３）、通信がなされないと判別したときにはステップＳ１６２に戻る。

【０２１２】

また、ステップＳ１６３で、玄関ドア施錠後、所定時間経過する前に、ステップＳ５１において通信が行われたと判別された電子鍵装置と外側電子鍵リード／ライト部２１ｅｘとで通信が行われたと判別すると、戸締りを確認する（ステップＳ１６４）。

【０２１３】

このステップＳ１６４での戸締りの確認は、前述のステップＳ６１～Ｓ６３において説明した処理と同様に行なう。つまり、ドアロック制御装置１００は、監視制御装置３に対して窓の開閉状態についての問い合わせを行ない、問い合わせ結果を監視制御装置３から取得する。そして、その問い合わせ結果から、戸締りがＯＫかどうかを判別する。

【０２１４】

ステップＳ１６４で、戸締りがＯＫであると判別したときには、ＣＰＵ１０１は、通信インターフェース１２１を通じてセキュリティモードをオンにする要求を監視制御装置３に送信する（ステップＳ１６５）。

【０２１５】

この要求に対しては、監視制御装置３は、そのときの在宅状況をチェックして、セキュリティレベルが図１１に示したいずれのレベルとなるかを判定する。そして、監視制御装置３は、その判定の結果、セキュリティレベルがレベルＤであるときには、セキュリティモードはオンにできないので、その旨をドアロック制御装置１００に返し、セキュリティレベルがレベルＤ以外であるときには、セキュリティモードをオンにできるので、その旨をドアロック制御装置１００に返す。

【０２１６】

ドアロック制御装置１００のＣＰＵ１０１は、監視制御装置３からのセキュリティモードオンの要求に対する返答を解析して、セキュリティモードをオンにできるか否か判別する（ステップＳ１６６）。そして、セキュリティモードがオンにできる旨の返答を監視制御装置３から受けたと判別したときには、ＣＰＵ１０１は、外側スピーカ２３ｅｘから、「セキュリティモードをオンにします」というメッセージを放音させる（ステップＳ１６７）。

【０２１７】

また、ステップＳ１６６で、セキュリティモードがオンにできない旨の返答を監視制御装置３から受けたと判別したときには、ＣＰＵ１０１は、外側スピーカ２３ｅｘから、「在宅者が存在するため、セキュリティモードをオンにはできません」というメッセージを放音させる（ステップＳ１６８）。その後、ステップＳ１３１に戻る。

【０２１８】

また、ステップＳ１６４で、窓が開いていて戸締りが完了していないと判別したときには、ＣＰＵ１０１は、「窓が開いているため、セキュリティモードをオンにすることはできません」という警告メッセージを放音する（ステップＳ１６９）。そして、その後、ステップＳ１３１に戻る。

【０２１９】

［監視制御装置３におけるセキュリティ動作；図２６］

上述のようにして、監視制御装置３は、ドアロック制御装置１００からの指示を受けてセキュリティモードをオンにするが、リモートコマンダ５０のセキュリティボタン５１を押すことによってもセキュリティモードをオンにすることができる。そして、監視制御装置３のセキュリティモードオン状態は、リモートコマンダ５０のオフボタン５２を操作すると、オフとすることができる。

【０２２０】

図２６は、リモートコマンダ５０を操作することにより、監視制御装置３のセキュリティモードのオン・オフを制御する動作を説明するためのフローチャートである。

【０２２１】

まず、ＣＰＵ２０１は、リモートコマンダ５０からの遠隔操作信号を監視して、リモートコマンダ５０で操作入力がなされたか否か判別する（ステップＳ１７１）。そして、操作入力がなされたと判別したときには、ＣＰＵ２０１は、操作されたのはセキュリティボタン５１であるか否か判別する（ステップＳ１７２）。

【０２２２】

ステップＳ１７２での判別の結果、セキュリティボタン５１の操作であると判別したときには、ＣＰＵ２０１は、リモコン送信部３９から電源オンのリモコン信号をテレビ受像機７のリモコン受信部に送り、テレビ受像機７をオンにする（ステップＳ１７３）。

【０２２３】

そして、ＣＰＵ２０１は、ＲＯＭ２０３から読み出したデータに基づいて生成した画像情報を、テレビインターフェース２１７を通じてテレビ受像機７に送り、テレビ受像機７の画面にセキュリティモードオンの確認画面を表示する（ステップＳ１７４）。その後、ＣＰＵ２０１は、リモコン送信部３９からテレビ受像機７の電源をオフするリモコン信号を送出して、テレビ受像機７をオフさせる（ステップＳ１７５）。

【０２２４】

そして、ＣＰＵ２０１は、その所定時間、例えば５分経過後、セキュリティモードをオンにして（ステップＳ１７７）、セキュリティ監視動作を実行する（ステップＳ１７８）。ステップＳ１７７における所定時間は、セキュリティボタン５１を操作した使用者が、セキュリティモードオンに設定した後、玄関ドアから退出するまでの時間を考慮した時間とされている。

【０２２５】

ステップＳ１７２において、リモートコマンダ５０で操作されたボタンがセキュリティボタン５１ではないと判別したときには、ＣＰＵ２０１は、操作されたのはオフボタン５２であるか否か判別する（ステップＳ１７９）。このステップＳ１７９でオフボタン５２ではないと判別したときには、ＣＰＵ２０１は、その他のボタンが押されたことによる処理を実行する（ステップＳ１８０）。

【０２２６】

ステップＳ１７９での判別の結果、オフボタン５２であると判別したときには、ＣＰＵ２０１は、リモコン送信部３９から電源オンのリモコン信号をテレビ受像機７のリモコン受信部に送り、テレビ受像機７をオンにする（ステップＳ１８１）。

【０２２７】

そして、ＣＰＵ２０１は、ＲＯＭ２０３から読み出したデータに基づいて生成した画像情報を、テレビインターフェース２１７を通じてテレビ受像機７に送り、テレビ受像機７の画面にセキュリティモードオフの確認画面を表示する（ステップＳ１８２）。その後、ＣＰＵ２０１は、リモコン送信部３９からテレビ受像機７の電源をオフするリモコン信号を送出して、テレビ受像機７をオフさせる（ステップＳ１８３）。

【０２２８】

そして、ＣＰＵ２０１は、セキュリティモードをオフにする処理を行なう（ステップＳ１８４）。以上で、図２６の処理ルーチンは終了となる。

【０２２９】

[セキュリティモードオンにおける監視動作]

図２７および図２８は、監視制御装置３において、セキュリティモードオンとされたときの処理動作である。これは、前述のリモートコマンダ５０でのセキュリティボタン５１の操作時に起動されるもので、このときのセキュリティレベルは、レベルＡの場合である。なお、ドアロック制御装置１００からのセキュリティモードオン指示があったときには、前述したように、在宅者の状況が参酌されてセキュリティレベルが決定され、その決定されたセキュリティレベルでセキュリティモードがオンとされるものである。

【０２３０】

図２７においては、先ず、ＣＰＵ２０１は、ビデオカメラ３１の撮影画像の取り込みを開始する（ステップＳ１９１）。このとき、マイクロホン３４で収音した音声も一緒に取り込みを行なう。前述したように、画像・音声メモリ２０８に設けられるセキュリティモード用の監視情報領域は、リングバッファ形式とされており、この例では、最新の３０秒分の画像・音声情報が常に画像・音声メモリ２０８に格納されるようにされている。監視カメラ１３からの撮影画像についても同様にされている。

【０２３１】

次に、ＣＰＵ２０１は、センサハブ２０７からの窓センサ１６ａ、１６ｂのセンサ出力と、玄関ドア１のドア開閉センサ２７のセンサ出力の監視を開始するよ

うに制御する（ステップＳ１９２）。さらに、ＣＰＵ２０１は、火災センサ４およびガスセンサ５のセンサ出力の監視を開始するように制御する（ステップＳ１９３）。監視カメラ１３は、火災センサ４やガスセンサ５のオン・オフに応じてオン・オフする。

【０２３２】

次に、ＣＰＵ２０１は、人感センサ３３のセンサ出力を監視して、侵入者がないかどうかチェックする（ステップＳ１９４）。侵入者なしと判別したときには、窓センサ１６ａ，１６ｂのセンサ出力や、ドア開閉センサ２７のセンサ出力から、異常を検知したか否か判別する（ステップＳ２１１）。

【０２３３】

ステップＳ２１１で、異常を検知しないと判別したときには、ＣＰＵ２０１は、火災センサ４やガスセンサ５のセンサ出力から、異常を検知したか否か判別する（ステップＳ２１２）。ステップＳ２１２で、異常を検知しないと判別したときには、ステップＳ１９４に戻る。

【０２３４】

そして、ステップＳ１９４で、侵入者を人感センサ３３により検知したと判別したときには、ＣＰＵ２０１は、照明機構３２０を制御して、照明３２をオンにする（ステップＳ１９５）。そして、侵入者の検知時点の１０秒前から、検知時点の２０秒後までの３０秒分の画像・音声情報を、画像・音声メモリ２０８から読み出し、１回目の画像として、管理サーバ装置１０に転送する（ステップＳ１９６）。管理サーバ装置１０では、この転送されてきた画像・音声情報により、侵入者を認識して、適切な処置を取ることができる。

【０２３５】

次に、ＣＰＵ２０１は、リモコン送信部３９からテレビ受像機７に電源オンのリモコン信号を送り、テレビ受像機７をオンにする（ステップＳ１９７）。そして、ＣＰＵ２０１は、予め用意している威嚇画像および威嚇音声の情報をテレビ受像機７に送り、それら威嚇画像および威嚇音声を出力する（ステップＳ１９８）。この威嚇画像・音声により侵入した賊を威嚇して、退散させることが可能となる。

【０２３６】

次に、ＣＰＵ２０１は、監視制御装置３に予め登録されている連絡先、例えば警備会社、警察署の他、登録された家人の携帯電話に対して異常検知を連絡する（ステップＳ１９９）。

【０２３７】

そして、ＣＰＵ２０１は、その後、数秒間隔で、画像・音声メモリ２０８のリングバッファに格納されている３０秒分の画像・音声情報を繰り返し管理サーバ装置１０に転送する（ステップＳ２００）。そして、ＣＰＵ２０１は、人感センサ３３が侵入者を検知しなくなったか否か判別し（ステップＳ２０１）、検知しなくなるまで、３０秒分の画像・音声情報を管理サーバ装置１０に転送する処理作業を継続する。

【０２３８】

そして、ＣＰＵ２０１は、人感センサ３３が侵入者を検知しなくなったと判別したときには、３０秒分の画像・音声情報の管理サーバ装置１０への転送を中止する（ステップＳ２０２）。そして、ステップＳ１９１に戻って、セキュリティ監視を続ける。

【０２３９】

また、ステップＳ２１１において、異常を検知したと判別したときには、ＣＰＵ２０１は、窓センサ６ａ，６ｂやドア開閉センサ２７の近傍に設置されている監視カメラ１３からの検知時点の１０秒前から、検知時点の２０秒後までの３０秒分画像を１回目として、管理サーバ装置１０に転送する（ステップＳ２１４）。

【０２４０】

そして、ＣＰＵ２０１は、リモコン送信部３９からテレビ受像機７に電源オンのリモコン信号を送り、テレビ受像機７をオンにする（ステップＳ２１５）。そして、ＣＰＵ２０１は、予め用意している威嚇画像および威嚇音声の情報をテレビ受像機７に送り、それら威嚇画像および威嚇音声を出力する（ステップＳ２１６）。この威嚇画像・音声により侵入した賊を威嚇して、退散させることが可能となる。

【０２４１】

次に、ＣＰＵ２０１は、監視制御装置３に予め登録されている連絡先、例えば警備会社、警察署の他、登録された家人の携帯電話に対して異常検知を連絡する（ステップＳ２１７）。

【０２４２】

そして、ＣＰＵ２０１は、その後、数秒間隔で、画像・音声メモリ２０８のリングバッファに格納されている３０秒分の画像・音声情報を繰り返し管理サーバ装置１０に転送する（ステップＳ２１８）。そして、ＣＰＵ２０１は、リモートコマンダ５０のオフボタン５２によるオフ指示を待ち（ステップＳ２１９）、オフ指示が有ったときには、セキュリティモードをオフとする。

【０２４３】

また、ステップＳ２１２で、火災センサ４またはガスセンサ５で異常が検知されたと判別したときには、ＣＰＵ２０１は、監視制御装置３に設定登録されている、例えば警備会社、消防署の他、登録された家人の携帯電話に対して異常検知を連絡する（ステップＳ２１３）。そして、ステップＳ２１９に進む。

【０２４４】

なお、画像・音声情報を監視制御装置３から受け取った管理サーバ装置１０は、Ｗｅｂページにそれらの画像・音声情報を載せる。そこで、監視制御装置３から連絡を受け取った携帯電話の持ち主は、管理サーバ装置１０の当該Ｗｅｂページにアクセスして、どのような異常が発生したかを知ることができ、適切な対応処置を講じることが可能になる。

【０２４５】

[監視制御装置３におけるドアロック制御装置１００からの指示による連携；図２９]

監視制御装置３のＣＰＵ２０１は、ドアロック制御装置１００から受け取った情報や指示に応じて、図２９に示すような連携動作を行なう。なお、この例は、セキュリティレベルの変更は、ＣＰＵ２０１が、ドアロック制御装置１００からの変更指示を受けて行なうのではなく、ドアロック制御装置１００からの個人情報を受け取った結果による在宅状況の変化をチェックして、必要に応じて行なう

ようにした場合である。

【０２４６】

すなわち、ＣＰＵ２０１は、ドアロック制御装置１００からセキュリティモードオンの指示を受け取ったか否か判別する（ステップＳ２２１）。受け取らないと判別したときには、ＣＰＵ２０１は、その他の処理を行なう（ステップＳ２２２）。

【０２４７】

ステップＳ２２１でセキュリティモードオンの指示を受信したと判別したときには、ＣＰＵ２０１は、家族情報メモリ２０５の記憶情報を参照して、在宅状況をチェックする（ステップＳ２２３）。そして、図１１に示したテーブルを参照して、在宅状況に応じたセキュリティレベルを認識し、セキュリティモードオンにすることが可能であるか否か判別する（ステップＳ２２４）。

【０２４８】

ステップＳ２２４で、セキュリティモードオンにすることができないと判別したときには、ＣＰＵ２０１は、その旨をドアロック制御装置１００に通知する（ステップＳ２２５）。

【０２４９】

一方、ステップＳ２２４で、セキュリティモードオンにすることが可能であると判別したときには、セキュリティモードをオンにすることができる旨をドアロック制御装置１００に通知し（ステップＳ２２６）、所定時間経過するのを待つ（ステップＳ２２７）。

【０２５０】

所定時間経過したことを確認したら、ＣＰＵ２０１は、在宅状況に応じたセキュリティレベルでセキュリティモードをオンにする（ステップＳ２２８）。そして、セキュリティ監視動作を開始する（ステップＳ２２９）。

【０２５１】

このセキュリティ監視動作中において、ドアロック制御装置１００から識別情報を含む個人情報を受信したか否か判別し（ステップＳ２３０）、受信しなければステップＳ２２９に戻って、セキュリティ監視動作を継続する。ドアロック制

御装置１００から個人情報を受信したと判別したときには、その結果としての在宅状況の変化をチェックし（ステップＳ２３１）、セキュリティレベルの変更が必要であるか判別する（ステップＳ２３２）。

【０２５２】

セキュリティレベルの変更が必要ではないと判別したときには、ＣＰＵ２０１は、ステップＳ２２９に戻って、セキュリティ監視動作を継続する。また、ステップＳ２３２で、セキュリティレベルの変更が必要であると判別したときには、変更の結果、セキュリティモードはオフにすべきものであるか否か判別し（ステップＳ２３３）、そうではないときには、在宅状況に応じてセキュリティレベルを変更する（ステップＳ２３４）。そして、セキュリティレベルを変更した旨をドアロック制御装置１００に通知する（ステップＳ２３５）。

【０２５３】

また、ステップＳ２３３で、セキュリティモードはオフにすべきものであると判別したときには、セキュリティモードをオフにし（ステップＳ２３６）、その旨をドアロック制御装置１００に通知する（ステップＳ２３７）。そして、ステップＳ２２１に戻る。

【０２５４】

以上のようにして、この実施形態によれば、非接触の電子鍵装置を用いて、施錠、開錠を行なうので、鍵穴がなく、いわゆるピッキング対策の防犯効果がある。

【０２５５】

また、ドアロック装置２を、オートロックモードと、逐次ロックモードとで使い分けることができるので、使用者が、自分の使い勝ってに合わせて、いずれのモードにするかを選択することができて、非常に便利である。

【０２５６】

また、内側電子鍵リード／ライト部２１ｉｎを設けて、この内側電子鍵リード／ライト部２１ｉｎによっても、ドアのロック状態を電子鍵装置により制御することができるので、窓などから侵入した不審者が玄関ドアから退出するのを妨げることができる。

【０２５７】

また、内側電子鍵リード／ライト部２１ｉｎと、外側電子鍵リード／ライト部２１ｅｘとを設けることにより、これらと電子鍵装置との通信により、家族の入退出の管理をすることが容易である。

【０２５８】

そのため、ドアロック装置２と、監視制御装置３とを組み合わせることにより、効率的なセキュリティ管理をすることができるようになる。そして、セキュリティモードをドアロック時に設定できるようにしているので、従来は、家の中で設定して、所定時間後に、家の外に出なければならないなどのあわただしさを解消することができる。

【０２５９】

また、窓の閉め忘れがあったときには、ドアの開閉時に確認されるので、窓の閉め忘れを防止することができる。

【０２６０】

また、家人の年齢、性別などにより、セキュリティモードのレベルを可変することができるようにしたので、在宅者が弱者である場合にも効果的なセキュリティレベルを設定することができる。また、ドアロックの開錠、施錠に連携して、在宅状況の変化を把握することにより、セキュリティレベルの変更をすることができるというメリットもある。

【０２６１】

[電子鍵装置の電子鍵情報の登録]

この電子鍵情報としての識別情報の登録が簡単にできることはセキュリティの点で好ましくないので、この例では、この電子鍵情報としての識別情報の登録は、次のようにセキュリティを重視した方法により、例えばドアロック装置２の販売業者あるいは設置業者もしくは使用者により行なわれる。

【０２６２】

先ず、本鍵情報の登録について説明する。この実施形態においては、前述したように、初期的な本鍵情報となる識別情報を記憶する電子鍵装置は、ＩＣカードとしており、ドアロック装置２の販売業者あるいは設置業者から、ドアロック装

置２の各戸への設置に際して、使用者に渡される。

【０２６３】

この実施形態の場合、ドアロック装置２の各戸への設置前に、当該ドアロック装置２を設置する戸の家族構成員の各人についての個人情報が収集される。そして、当該家族構成員の各人に対して、本鍵情報となる識別情報を記憶するＩＣカードが割り当てられ、それぞれのＩＣカードに記憶される本鍵情報としての識別情報と、前記収集された個人情報とからなる個人プロファイル情報が構成される。

【０２６４】

そして、設置されるドアロック装置２のシリアル番号等からなる製品番号、設置される住所、電話番号、ドアロック装置を利用する家族構成員の氏名などのユーザ情報と、各家族構成員の前記個人プロファイル情報が、予め管理サーバ装置１０のドアロック装置管理データベース３０５に、記憶される。すなわち、家族構成員それぞれの本鍵情報は、各家族構成員の個人プロファイル情報と関連付けられて予め管理サーバ装置１０に登録されている。

【０２６５】

管理サーバ装置１０に登録された本鍵情報および各家族構成員の個人プロファイル情報は、ドアロック装置２の設置業者や販売業者が、ドアロック装置２の設置を完了したときに、管理会社の管理サーバ装置１０に初期登録要求をしたときに、管理サーバ装置１０から監視制御装置３に転送されることにより、監視制御装置３の家族情報メモリ２０５に書き込まれて登録される。また、監視制御装置３に登録された情報のうち、少なくとも本鍵情報は、ドアロック制御装置１００に転送されることにより、その家族情報メモリ１２０登録される。

【０２６６】

図３０は、初期登録要求を受けたときの管理サーバ装置１０の動作を示すものである。図３０の各ステップの動作は、主としてＣＰＵ３０１が主体となって行なうものである。

【０２６７】

先ず、ＣＰＵ３０１は、初期登録要求を受け付けたか否か判別する（ステップ

Ｓ２４１）。この初期登録要求は、ドアロック装置２のシリアル番号等の装置識別情報を伴ったものとされているもので、例えばパーソナルコンピュータなどから通信ネットワークを通じて管理サーバ装置１０に送られる場合と、電話等で、初期登録要求を受けたオペレータが図示しない入力手段により入力する場合とがある。

【０２６８】

ＣＰＵ３０１は、この初期登録要求を受け取ると、装置識別情報を検索子として、ドアロック装置データベースを検索し、予め登録されている電話番号を読み出して、初期登録要求を含む発呼をする。つまり、初期登録要求されたドアロック装置２が接続されている監視制御装置３に対して初期登録要求の発呼を行なう（ステップＳ２４２）。

【０２６９】

このとき、監視制御装置３は、自動応答を行なうので、ＣＰＵ３０１は、当該監視制御装置３からの応答を確認して、当該監視制御装置３との間に通信路を形成する（ステップＳ２４３）。

【０２７０】

次に、ＣＰＵ３０１は、ドアロック装置２に関連して上述のように管理サーバ装置１０のドアロック装置データベース２０５に記憶している、ドアロック装置が設置された家の家族構成員全員についての本鍵情報を含む個人プロファイル情報を監視制御装置３に送信する（ステップＳ２４４）。

【０２７１】

次に、ＣＰＵ３０１は、監視制御装置３に送信すべき情報が全部終了し終わり、監視制御装置３から登録完了通知が到来するのを待ち（ステップＳ２４５）、登録完了通知を受け取ったと判別したときには、監視制御装置３との通信路を切断して（ステップＳ２４６）、この初期登録の処理ルーチンを終了する。

【０２７２】

この初期登録要求情報を受け取る監視制御装置３の動作を、図３１のフローチャートを参照して説明する。

【０２７３】

監視制御装置３のＣＰＵ２０１は、管理サーバ装置１０からの着信を受信したか否か判別し（ステップＳ２５１）、管理サーバ装置１０からの着信の受信でなかったと判別したときには、その他の処理を行なう（ステップＳ２５２）。

【０２７４】

管理サーバ装置１０からの着信を受信したと判別したときには、ＣＰＵ２０１は、その着信に自動応答して管理サーバ装置１０との間に通信路を形成する（ステップＳ２５３）。そして、受信した着信は初期登録要求であるか否か判別する（ステップＳ２５４）。初期登録要求であると判別すると、ＣＰＵ２０１は、管理サーバ装置１０からの登録情報を待ち、登録情報を受信したら（ステップＳ２５５）、受信した登録情報を、家族情報メモリ２０５に書き込む（ステップＳ２５６）。

【０２７５】

そして、家族全員についての登録情報の書き込みが完了したら、管理サーバ装置１０に登録完了通知を返送し（ステップＳ２５７）、管理サーバ装置１０との通信路を切断する（ステップＳ２５８）。

【０２７６】

次に、ＣＰＵ２０１は、家族情報メモリ２０５に書き込んで登録した個人プロファイル情報のうち、少なくとも家族構成員のそれぞれについての本鍵情報である識別情報をドアロック制御装置１００に転送する（ステップＳ２５９）。ドアロック制御装置１００は、この情報を受けて、家族情報メモリ１２０に受信した本鍵情報を登録する。本鍵情報としての識別情報のほかに、家族構成員についての個人情報の必要なものをも、ドアロック制御装置１００に転送するようにしてもよいことは言うまでもない。なお、ドアロック制御装置１００での登録動作は、上述の監視制御装置での鍵登録動作と同様であるので、ここでは省略する。

【０２７７】

そして、ＣＰＵ２０１は、ドアロック制御装置１００への本鍵情報および必要は情報の転送の終了を確認すると（ステップＳ２６０）、この処理ルーチンを終了する。

【０２７８】

なお、ステップＳ２５４で、初期登録ではないと判別したときには、ＣＰＵ２０１は、後述するバックアップ鍵の登録要求であるか否か判別し（ステップＳ２６１）、バックアップ鍵の登録要求であると判別したときには、当該バックアップ登録の処理を実行する（ステップＳ２６２）。このバックアップ登録の処理については後述する。

【０２７９】

また、ステップＳ２６１でバックアップ登録要求ではないと判別したときには、ＣＰＵ２０１は、紛失鍵の抹消要求であるか否か判別する（ステップＳ２６３）。そして、紛失鍵の抹消要求でないと判別したときには、ＣＰＵ２０１は、その他の処理を実行し（ステップＳ２６４）、紛失鍵の抹消要求であると判別したときには、当該抹消要求の処理を実行する（ステップＳ２６５）。以上で、図３１の処理を終了する。

【０２８０】

[バックアップ鍵登録について]

この実施形態においては、管理サーバ装置１０が備える鍵登録ホームページにアクセスすることにより、バックアップ鍵の登録を行なうことができる。図３２は、このバックアップ鍵登録の際のシステム構成を説明するための図である。また、図３３および図３４は、このときの管理サーバ装置１０の動作を説明するためのフローチャートである。

【０２８１】

図３２に示すように、先ず、電子鍵リード／ライト装置２００１を備える、あるいは電子鍵リード／ライト装置２００１が接続されているパーソナルコンピュータ２００２を用意する。そして、電子鍵リード／ライト装置２００１にバックアップ鍵として登録したい電子鍵装置、例えばＩＣカード、携帯電話端末、ＰＤＡをセットする。これらの電子鍵装置は、前述したように、本鍵情報が格納されたＩＣカード４０Ｃの識別情報と異なるように一元管理されたＩＣチップおよび電磁誘導アンテナなどからなる通信手段を備えるものである。

【０２８２】

次に、パーソナルコンピュータ２００２からインターネット２００３を通じて

管理サーバ装置１０の鍵登録ホームページにアクセスする。

【０２８３】

管理サーバ装置１０では、この鍵登録ホームページへのアクセスの有無を監視しており（ステップＳ２７１）、アクセスがないときには、その他の処理を行なっている（ステップＳ２７２）。そして、鍵登録ホームページへのアクセスを受信したときには、ＣＰＵ３０１は、鍵登録ホームページの表示情報を送信する（ステップＳ２７３）。

【０２８４】

この鍵登録ホームページは、パーソナルコンピュータ２００２の画面に表示される。この画面には、登録者の認証確認用情報の入力を促すメッセージと、入力欄が表示されているので、予め定められたパスワードや顧客ＩＤ、ドアロック装置２が設置された住所、電話番号、鍵登録を要求している者の氏名などの必要な認証確認用情報を入力した後、当該認証確認用情報を管理サーバ装置１０に送る。

【０２８５】

管理サーバ装置１０では、この認証確認用情報を受信したか否か判別し（ステップＳ２７４）、受信したら認証がＯＫであるか否か判別する（ステップＳ２７５）。認証が取れなかったとき（認証ＮＧのとき）には、認証ＮＧを報知する画面をパーソナルコンピュータ２００２に送る（ステップＳ２７６）。

【０２８６】

この認証ＮＧを報知する画面では、認証確認用情報の再入力をすることができると共に、アクセスを中断することもできる。鍵登録者は、いずれかの操作をすることになる。

【０２８７】

そこで、管理サーバ装置１０のＣＰＵ３０１は、認証確認用の情報を再受信したか否か判別し（ステップＳ２７７）、再受信しなかったときには、アクセスが中断されたかどうか判別し（ステップＳ２７８）、アクセス中断と判別されなかったときには、ステップＳ２７７に戻る。そして、ステップＳ２７７で、認証確認用の情報を再受信したと判別したときには、ＣＰＵ３０１は、ステップＳ２７

５に戻って、認証が取れるかどうか判別する。ステップＳ２７８で中断であると判別したときには、アクセス切断処理を行なう（ステップＳ２７９）。

【０２８８】

ステップＳ２７５において、認証がＯＫであると判別したときには、ＣＰＵ３０１は、バックアップ鍵登録用画面を送信する（ステップＳ２８１）。このバックアップ鍵登録用画面には、鍵登録ボタンと、アクセス中断ボタンがある。鍵登録者は、いずれかのボタンを操作することになる。鍵登録ボタンが押されたときには、パーソナルコンピュータ２００２は、バックアップ登録したい電子鍵装置４０Ｂから電子鍵リード／ライト部２００１により識別情報を読み取って、バックアップ鍵情報として管理サーバ装置１０に送る。

【０２８９】

そこで、管理サーバ装置１０のＣＰＵ３０１は、バックアップ鍵情報を受信したか否か判別し（ステップＳ２８２）、受信しなかったときには、アクセスが中断されたかどうか判別し（ステップＳ２８３）、アクセス中断と判別されなかったときには、ステップＳ２８２に戻る。

【０２９０】

そして、ステップＳ２８３で中断であると判別したときには、アクセス切断処理を行なって（ステップＳ２７９）、鍵ホームページを閉じる。また、ステップＳ２８２で、バックアップ鍵情報を受信したと判別したときには、ＣＰＵ３０１は、ドアロック装置データベース３０５に、鍵登録要求者のバックアップ鍵情報として、受信した電子鍵情報を登録する（ステップＳ２８５）。このとき、電子鍵登録・紛失履歴メモリ３０６にも、その登録したバックアップ鍵情報と、鍵登録要求者の識別情報とがバックアップ登録履歴として、カレンダー情報および時刻情報と共に書き込まれる。

【０２９１】

そして、アクセス切断を行なった後（ステップＳ２８６）、鍵登録要求者が登録されているドアロック装置２が接続されている監視制御装置３に、バックアップ鍵登録要求の発信を行なう（ステップＳ２８７）。監視制御装置３では、このバックアップ鍵登録要求の発信の着信を受けると、その着信に自動応答するので

、ＣＰＵ３０１は、当該監視制御装置３との間に通信路を形成する（ステップＳ２８８）。

【０２９２】

次に、ＣＰＵ３０１は、鍵登録要求者を識別する情報と、バックアップ鍵情報とを監視制御装置３に送信する（ステップＳ２８９）。次に、ＣＰＵ３０１は、監視制御装置３に送信すべき情報が全部終了し終わり、監視制御装置３から登録完了通知が到来するのを待ち（ステップＳ２９０）、登録完了通知を受け取ったと判別したときには、監視制御装置３との通信路を切断して（ステップＳ２９１）、このバックアップ鍵登録の処理ルーチンを終了する。

【０２９３】

次に、前記ステップＳ２８７～ステップＳ２８９での送信動作により管理サーバ装置１０から送られてくるバックアップ鍵情報を受け取る監視制御装置３の動作を、図３５のフローチャートを参照して説明する。この処理ルーチンは、図３１におけるステップＳ２６２の処理に相当する。

【０２９４】

監視制御装置３のＣＰＵ２０１は、まず、バックアップ鍵情報と、鍵登録要求者の名前などの識別情報とを受信し（ステップＳ３０１）、鍵登録要求者を認識する（ステップＳ３０２）。次に、受信したバックアップ鍵情報を、認識した登録要求者のバックアップ鍵情報として、家族情報メモリ２０５に書き込んで登録する（ステップＳ３０３）。

【０２９５】

このとき、当該鍵登録要求者の個人プロファイル情報の電子鍵登録・紛失履歴エリアに、その登録したバックアップ鍵情報とカレンダー情報および時刻情報とがバックアップ登録履歴として書き込まれる。

【０２９６】

そして、ＣＰＵ２０１は、管理サーバ装置１０に、バックアップ鍵情報の登録完了通知を送る（ステップＳ３０４）。そして、管理サーバ装置１０との通信路を切断する（ステップＳ３０５）。

【０２９７】

次に、ＣＰＵ２０１は、家族情報メモリ２０５に書き込んで登録したバックアップ鍵情報である識別情報を、鍵登録要求者の識別情報と共に、ドアロック制御装置１００に転送する（ステップＳ３０６）。ドアロック制御装置１００は、この情報を受けて、家族情報メモリ１２０に、受信したバックアップ鍵情報を登録する。そして、ＣＰＵ２０１は、ドアロック制御装置１００への本鍵情報および必要は情報の転送の終了を確認すると（ステップＳ３０７）、この処理ルーチンを終了する。

【０２９８】

なお、ドアロック制御装置１００における電子鍵情報の認証には本鍵情報のみを用いるようにする場合には、ステップＳ３０６およびステップＳ３０７の処理は、行なわなくてもよい。つまり、ドアロック制御装置１００には、常に本鍵情報が存在すればよいからである。その場合には、後述する紛失鍵抹消登録の際に、紛失鍵情報の抹消と共に、新たに本鍵情報として使用する、予め監視制御装置３にバックアップ登録されていた鍵情報が、監視制御装置３からドアロック制御装置１００に転送されるようにされる。

【０２９９】

なお、ドアロック制御装置１００での登録動作は、上述の監視制御装置での鍵登録動作と同様であるので、ここでは省略する。

【０３００】

なお、以上の電子鍵情報としての識別情報の登録動作は一例であって、例えばパーソナルコンピュータ２００２および電子鍵リード／ライト装置２００１の代わりに、監視制御装置３を用いて、同様にして管理サーバ装置１０にアクセスして、バックアップ鍵を登録するようにしても良い。

【０３０１】

また、管理サーバ装置１０を介することなく、監視制御装置３およびドアロック制御装置１００に、電子鍵情報としての識別情報を登録することができるようにしても良い。

【０３０２】

なお、バックアップ鍵登録の際の鍵登録者の認証のために、本鍵情報を管理サ

ーバ装置に送り、その後、バックアップ鍵登録したい電子鍵装置をセットして登録を行なうようにしてもよい。その場合には、鍵登録者の認証は、本鍵情報により行なうことができるので、上述の例における鍵登録者の認証確認用情報の入力は不要となる。

【０３０３】

［鍵の紛失対策］

電子鍵装置を紛失してしまった場合には、当該紛失した電子鍵装置の悪意の取得者の利用を防止するため、この実施形態では、電子鍵情報の抹消処理を行なうようにする。図３６は、本鍵情報の抹消処理を行なう場合のシステム構成を示す図である。また、図３７は、そのときの処理手順を説明するためのフローチャートである。

【０３０４】

まず、紛失者は、管理会社に対して紛失届を提出する（手順Ｓ３１１）。この紛失届は、電話やメールなどが用いられて行なわれる。この際に、紛失者の本人確認が行なわれ（手順Ｓ３１２）、本人確認がＯＫであったときに、紛失届が受理される（手順Ｓ３１３）。本人確認は、住所、氏名、年齢、電話番号、パスワード、顧客番号などにより行なわれる。

【０３０５】

次に、管理会社のオペレータは、管理サーバ装置１０に対して紛失鍵情報の抹消処理およびバックアップ鍵情報の本鍵情報への格上げの処理を行なう（手順Ｓ３１４）。管理サーバ装置１０のＣＰＵ３０１は、紛失鍵情報の抹消処理およびバックアップ鍵情報の本鍵情報への格上げの処理を完了すると、電子鍵登録・紛失履歴メモリ３０６に、その抹消したバックアップ鍵情報と、抹消要求者の識別情報とを、電子鍵抹消履歴として、カレンダー情報および時刻情報と共に書き込む。

【０３０６】

また、管理サーバ装置１０のＣＰＵ３０１は、紛失鍵情報の抹消処理およびバックアップ鍵情報の本鍵情報への格上げの処理、抹消履歴の書き込みを完了すると、鍵紛失届を出した者が登録されているドアロック装置２が接続されている監

視制御装置３を、データベース３０５から検索して、自動的に、当該監視制御装置３にアクセスして、紛失鍵の抹消要求を送る（手順Ｓ３１５）。

【０３０７】

紛失鍵の抹消要求を受信した監視制御装置３は、紛失鍵情報の抹消処理およびバックアップ鍵情報の本鍵情報への格上げの処理を行なう。そして、監視制御装置３は、紛失鍵情報の抹消処理およびバックアップ鍵情報の本鍵情報への格上げの処理を完了すると、個人プロファイル情報の電子鍵登録・抹消履歴エリアに抹消履歴を書き込み、その後、ドアロック装置２に対して紛失鍵の抹消指示をする。そして、バックアップ鍵が登録されていれば、当該バックアップ鍵の格上げ処理も指示する（手順Ｓ３１６）。

【０３０８】

ドアロック装置２は、指示に従い、紛失鍵情報の抹消およびバックアップ鍵情報の格上げ処理を実行する（手順Ｓ３１７）。

【０３０９】

なお、前述もしたように、ドアロック制御装置１００における電子鍵情報の認証には本鍵情報のみを用いるようにする場合には、バックアップ鍵は、ドアロック制御装置１００には登録されない。その場合には、手順Ｓ３１６では、紛失鍵の抹消指示と共に、監視制御装置３にバックアップ登録されている鍵情報を本鍵情報として、ドアロック制御装置１００に送る。

【０３１０】

そして、その場合、ドアロック制御装置１００では、手順Ｓ３１７において、抹消指示を受けた鍵情報を抹消すると共に、その代わりに新たに受信した本鍵情報の登録を行なうことになる。

【０３１１】

図３８を参照して、手順Ｓ３１４および手順Ｓ３１５における管理サーバ装置１０の動作を説明する。

【０３１２】

管理会社のオペレータは、管理サーバ装置１０に対して紛失鍵の抹消要求者に関する情報を入力して、紛失鍵の抹消要求を入力する。管理サーバ装置１０のＣ

ＰＵ３０１は、この紛失鍵の抹消要求が入力されたか否か判別する（ステップＳ３２１）。ＣＰＵ３０１は、抹消要求がなければ、その他の処理を行なう（ステップＳ３２２）。

【０３１３】

ステップＳ３２１で、紛失鍵の抹消要求が入力されたと判別したときには、ＣＰＵ３０１は、ドアロック装置データベース３０５において抹消要求者および紛失鍵の情報を検索し（ステップＳ３２３）、抹消要求者の紛失鍵の情報を抹消すると共に、前述したように、電子鍵登録・紛失履歴メモリ３０６に紛失者および紛失鍵の情報を書き込む（ステップＳ３２４）。

【０３１４】

次に、ＣＰＵ３０１は、抹消要求者の電子鍵情報としては、バックアップ鍵情報が登録されているかどうか判別し（ステップＳ３２５）、バックアップ鍵情報が登録されていると判別したときには、登録されているバックアップ鍵情報を本鍵情報に登録しなおす（ステップＳ３２６）。そして、抹消要求者が登録されている監視制御装置３を、データベース３０５から検索して、当該監視制御装置３に紛失鍵の抹消要求の発信を行なう（ステップＳ３２７）。ステップＳ３２５で、バックアップ鍵情報が登録されていないと判別したときには、ステップＳ３２７に即座に進む。

【０３１５】

監視制御装置３では、このバックアップ鍵登録要求の発信の着信を受けると、その着信に自動応答するので、ＣＰＵ３０１は、当該監視制御装置３との間に通信路を形成する（ステップＳ３２８）。

【０３１６】

次に、ＣＰＵ３０１は、抹消要求者を識別する情報と、抹消すべき紛失鍵の情報とを監視制御装置３に送信する（ステップＳ３２９）。次に、ＣＰＵ３０１は、監視制御装置３に送信すべき情報が全部終了し終わり、監視制御装置３から抹消完了通知が到来するのを待ち（ステップＳ３３０）、抹消完了通知を受け取ったと判別したときには、監視制御装置３との通信路を切断して（ステップＳ３３１）、この紛失鍵情報の抹消処理ルーチンを終了する。

【０３１７】

次に、前記手順Ｓ３１６において、管理サーバ装置１０から送られてくる紛失鍵の抹消要求を受け取ったときの監視制御装置３の動作を、図３９のフローチャートを参照して説明する。この処理ルーチンは、図３１におけるステップＳ２６５の処理に相当する。

【０３１８】

監視制御装置３のＣＰＵ２０１は、まず、紛失鍵情報と、抹消要求者の名前などの識別情報とを受信し（ステップＳ３４１）、抹消要求者および紛失鍵情報を認識する（ステップＳ３４２）。次に、認識した抹消要求者の紛失鍵情報を、家族情報メモリ２０５から抹消する（ステップＳ３４３）。そして、抹消要求者の個人プロファイル情報中の電子鍵登録・抹消履歴情報として、抹消した電子鍵情報としての識別情報および日付、時刻等を、家族情報メモリ２０５に書き込んだ後、管理サーバ装置１０に、抹消完了通知を送る（ステップＳ３４４）。そして、管理サーバ装置１０との通信路を切断する（ステップＳ３４５）。

【０３１９】

次に、ＣＰＵ２０１は、抹消要求者の電子鍵情報としては、バックアップ鍵情報が登録されているかどうか判別し（ステップＳ３４６）、バックアップ鍵情報が登録されていると判別したときには、登録されているバックアップ鍵情報を本鍵情報に登録しなおす（ステップＳ３４７）。そして、ドアロック制御装置１００に紛失鍵の抹消指示を送る（ステップＳ３４８）。ステップＳ３４６で、バックアップ鍵情報が登録されていないと判別したときには、ステップＳ３４８に即座に進む。

【０３２０】

ドアロック制御装置１００では、抹消指示に従って、紛失鍵情報の抹消を実行した後、抹消完了通知を監視制御装置３に送る。そこで、監視制御装置３は、抹消完了通知の受信を待って（ステップＳ３４９）、この処理ルーチンを終了する。

【０３２１】

なお、ドアロック制御装置１００における電子鍵情報の認証には本鍵情報のみ

を用いるようにする場合には、バックアップ鍵情報が存在するときには、ステップＳ３４８では、紛失鍵の情報と共に、本鍵情報に格上げするバックアップ鍵情報を送るようにする。本鍵情報に格上げするバックアップ鍵情報は、抹消完了の後に、監視制御装置３から、ドアロック制御装置１００に送るようにしてもよい。

【０３２２】

なお、ドアロック制御装置１００での登録動作は、上述の監視制御装置での鍵登録動作と同様であるので、ここでは省略する。

【０３２３】

[他の実施形態]

上述の実施形態は、セキュリティ監視システムも含む通信システムの構成であったので、管理サーバ装置１０が存在しているが、セキュリティ監視システムが存在しない通信システムの構成も可能である。

【０３２４】

その場合には、監視制御装置３で行なえる機能に、バックアップ鍵登録や紛失鍵抹消を用意する。そして、リモートコマンダ５０により、メニューからそれらの機能を選択して、バックアップ鍵登録や、紛失鍵の抹消を行なうようにする。

【０３２５】

例えば、バックアップ鍵情報の登録は、リモートコマンダ５０により、メニューからバックアップ鍵登録を選択し、監視制御装置３に対して、バックアップ鍵情報を登録したい電子鍵装置をかざし、リモートコマンダ５０により、登録要求者の入力を行ない、登録実行を選択することにより、行なうことができる。

【０３２６】

鍵情報の抹消も同様にして、監視制御装置３において行なうことができる。この例の場合にも、監視制御装置３からドアロック制御装置１００に鍵情報を転送したり、抹消指示をしたりするのは、上述の場合と同様である。

【０３２７】

また、ドアの施錠および開錠のみを目的とするドアロック制御システムとして考えた場合には、監視制御装置３は不要である。その場合には、ドアロック制御

装置１００に対して、バックアップ鍵情報の登録を行なったり、紛失鍵情報の抹消を行なったりすることができる構成とすればよい。

【０３２８】

上述の例では、バックアップ鍵情報が登録されていても、本鍵情報のみを電子鍵装置からの識別情報の受信時の認証用としたが、家族情報メモリ１２０または２０５に登録されているバックアップ鍵情報をも含む全てを認証用として、常時、用いるようにしても勿論よい。

【０３２９】

その場合には、鍵紛失による抹消は、当該鍵情報の抹消を行なうだけでよく、上述の例のように、バックアップ鍵を本鍵情報に格上げするようにする処理は不要となる。

【０３３０】

なお、上述の実施形態では、本鍵情報は、予め管理サーバ装置にドアロック装置の設置会社や販売会社などにより、登録しておくようにしたが、本鍵情報もバックアップ情報と同様にして、上述のようにして後から登録することができるようにしてもよい。

【０３３１】

また、上述の実施形態では、パーソナルコンピュータを用いてバックアップ鍵の登録を行なうようにしたが、監視制御装置３から管理サーバ装置１０にアクセスすることにより、行なうこともできる。その場合には、監視制御装置３が備える電子鍵リード／ライト部３６を利用することができるので、電子鍵リード／ライト装置を別個に用意する必要はない。

【０３３２】

また、パーソナルコンピュータの代わりに、電子鍵リード／ライト装置に接続される携帯電話端末から、管理サーバ装置のホームページにアクセスして、バックアップ鍵登録を行なうようにすることもできる。

【０３３３】

また、上述の実施形態では、電子鍵情報の紛失届による抹消は、本鍵情報について説明したが、紛失届の際に、本鍵情報の紛失届か、バックアップ鍵情報の紛

失届かの指定をすることにより、バックアップ鍵情報の紛失届およびそれに基づくバックアップ鍵情報の抹消処理をすることもできる。

【０３３４】

また、ＩＣチップのメモリには、予め一元管理された識別情報が記憶されているように説明したが、後から、一元管理されている識別情報が書き込まれるようにされてもよいことは言うまでもない。

【０３３５】

なお、上述の実施形態では、電子鍵装置を、外側電子鍵リード／ライト部２１ｅｘに対して、ドアの施錠後、所定時間以内にかざした場合に、セキュリティモードをオンにするようにしたが、ドアロック制御装置１００または監視制御装置３では、玄関ドア１からの入退出を管理しているので、在宅者が無くなったら、自動的にセキュリティレベルＡでセキュリティモードをオンにするようにすることもできる。

【０３３６】

その場合に、ドアロック制御装置１００で、在宅者無しを検出したときに、監視制御装置３にセキュリティモードオンを要求しても良いし、監視制御装置３が、自装置で、在宅者無しを検出したときに、セキュリティモードオンとするようにしても良い。

【０３３７】

なお、この例では、在宅者が玄関ドア１を開錠し、玄関ドア１を開けたときには、それまでにセキュリティモードがオンになっていても、一旦、セキュリティモードは、オフとされるものとしたが、セキュリティモードがオンになっているときに外出者があった場合には、外出者を電子鍵装置との通信により取得される識別情報により認識して、監視制御装置３が、帰宅者があった場合と全く同様にして、在宅状況の変化に対応して自動的にセキュリティレベルを変更するようにすることもできる。

【０３３８】

なお、以上の実施形態の説明では、鍵情報としての識別情報の認証は、ドアロック装置で行なうようにしたが、ドアロック装置２は、監視制御装置３に、ある

いは監視制御装置３を介して管理サーバ装置１０に鍵情報を送り、監視制御装置３あるいは管理サーバ装置１０で、認証作業を行ない、その認証結果を、ドアロック装置２に返す（管理サーバ装置１０の場合には監視制御装置３を介して返す）ようにしても良い。その場合には、監視制御装置３からドアロック制御装置１００への鍵情報の転送や抹消指示を送る必要はない。

【０３３９】

また、開錠者、施錠者の識別情報も監視制御装置３ではなく、管理サーバ装置１０に送り、管理サーバ装置１０により、セキュリティ管理をするようにしてもよい。

【０３４０】

また、以上の説明では、外出者か帰宅者かは、ドアロック制御装置１００で判別するようにしたが、監視制御装置３においても、ドアロック制御装置１００でのドアロック制御モードの設定情報を備えているので、ドアロック制御装置１００は、電子鍵装置４０が、内側電子鍵リード／ライト部２１ｉｎまたは外側電子鍵リード／ライト部２１ｅｘにかざされて通信が両者の間で行なわれ、識別情報についての認証がとれたときには、その識別情報と、内側電子鍵リード／ライト部２１ｉｎまたは外側電子鍵リード／ライト部２１ｅｘのいずれと通信したかの情報と、開錠か施錠かの情報とを、監視制御装置３に送り、監視制御装置３が、外出か帰宅かを判別するようにすることもできる。

【０３４１】

また、電子鍵装置は、上述の実施形態のような非接触形式で電子鍵情報の通信を行なうのものに限られるものではなく、接触形式で電子鍵情報の通信を行なうものであっても勿論よい。

【０３４２】

【発明の効果】

以上説明したように、この発明によれば、同一のものが存在しないように一元管理された識別情報を電子鍵情報として用いることができるようにしたので、ドアの施錠、開錠に関するセキュリティを向上させることができる。

【０３４３】

また、前記識別情報は、同一のものが存在しないユニークなものであるので、これを使用者個人に対応させて管理することができる。その場合には、ドアからの入退出を個人レベルで管理することができ、在宅状況に応じたセキュリティ管理ができるなどの効果がある。

【図面の簡単な説明】

【図１】

この発明の実施形態の識別情報の概要を説明するための図である。

【図２】

この発明の実施形態で用いる識別情報の一例を示す図である。

【図３】

ドアロックシステムの実施形態を含むセキュリティシステムの概要を説明するための図である。

【図４】

ドアロックシステムの実施形態の要部を説明するための図である。

【図５】

実施形態のドアロック装置の構成例を示す図である。

【図６】

この発明の実施形態に用いる電子鍵装置の一例を示す図である。

【図７】

図６の電気的構成例を示す図である。

【図８】

セキュリティシステムに用いる監視制御装置の例を示す図である。

【図９】

図５の監視制御装置の構成例を示すブロック図である。

【図１０】

個人プロファイル情報の一例を示す図である。

【図１１】

セキュリティモードの内容を説明するための図である。

【図１２】

セキュリティモードの内容を説明するための図である。

【図１３】

管理サーバ装置の構成例を示すブロック図である。

【図１４】

図５の監視制御装置の伝言記録および再生機能を説明するためのフローチャートである。

【図１５】

ドアロック制御モードの設定動作を説明するためのフローチャートである。

【図１６】

ドアロック制御モードの設定動作を説明するためのフローチャートである。

【図１７】

ドアロック制御モードの一つの例であるオートロックモードでのドアロック制御動作を説明するためのフローチャートの一部である。

【図１８】

ドアロック制御モードの一つの例であるオートロックモードでのドアロック制御動作を説明するためのフローチャートの一部である。

【図１９】

ドアロック制御モードの一つの例であるオートロックモードでのドアロック制御動作を説明するためのフローチャートの一部である。

【図２０】

ドアロック制御モードの一つの例であるオートロックモードでのドアロック制御動作を説明するためのフローチャートの一部である。

【図２１】

ドアロック制御モードの一つの例であるオートロックモードでのドアロック制御動作を説明するためのフローチャートの一部である。

【図２２】

ドアロック制御モードの一つの例であるオートロックモードでのドアロック制御動作を説明するためのフローチャートの一部である。

【図２３】

ドアロック制御モードの一つの例である逐次ロックモードでのドアロック制御動作を説明するためのフローチャートの一部である。

【図２４】

ドアロック制御モードの一つの例である逐次ロックモードでのドアロック制御動作を説明するためのフローチャートの一部である。

【図２５】

ドアロック制御モードの一つの例である逐次ロックモードでのドアロック制御動作を説明するためのフローチャートの一部である。

【図２６】

監視制御装置のリモートコマンダからの信号の受信処理動作を説明するためのフローチャートである。

【図２７】

監視制御装置におけるセキュリティモードオン時の動作を説明するためのフローチャートの一部である。

【図２８】

監視制御装置におけるセキュリティモードオン時の動作を説明するためのフローチャートの一部である。

【図２９】

監視制御装置におけるドアロック装置との連携動作を説明するための図である。

【図３０】

この発明における実施形態において、本鍵情報の登録を説明するためのフローチャートを示す図である。

【図３１】

この発明における実施形態において、本鍵情報の登録を説明するためのシステム構成を示す図である。

【図３２】

この発明における実施形態において、バックアップ鍵情報の登録を説明するためのシステム構成を示す図である。

【図３３】

この発明における実施形態において、バックアップ鍵情報の登録を説明するためのフローチャートを示す図である。

【図３４】

この発明における実施形態において、バックアップ鍵情報の登録を説明するためのフローチャートを示す図である。

【図３５】

この発明における実施形態において、バックアップ鍵情報の登録を説明するためのフローチャートを示す図である。

【図３６】

この発明における実施形態において、紛失鍵情報の抹消を行なう場合のシステム構成を説明するための図である。

【図３７】

この発明における実施形態において、紛失鍵情報の抹消を行なう場合の手順を説明するための図である。

【図３８】

この発明における実施形態において、紛失鍵情報の抹消を説明するためのフローチャートを示す図である。

【図３９】

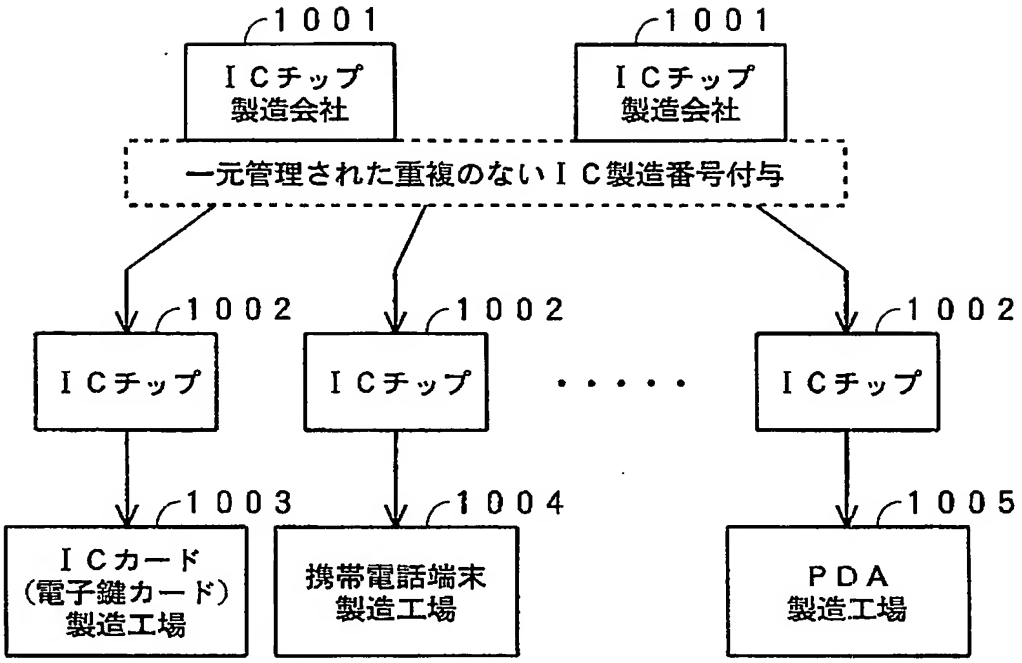
この発明における実施形態において、紛失鍵情報の抹消を説明するためのフローチャートを示す図である。

【符号の説明】

１…玄関ドア、２…ドアロック装置、３…監視制御装置、４…火災センサ、５…ガスセンサ、６ａ，６ｂ…窓センサ、７…テレビ受像機、８…電話回線、１０…管理サーバ装置１００…ドアロック制御装置、２１ｉｎ…内側電子鍵リード／ライト部、２１ｅｘ…外側電子鍵リード／ライト部、４０…電子鍵装置

【書類名】　図面

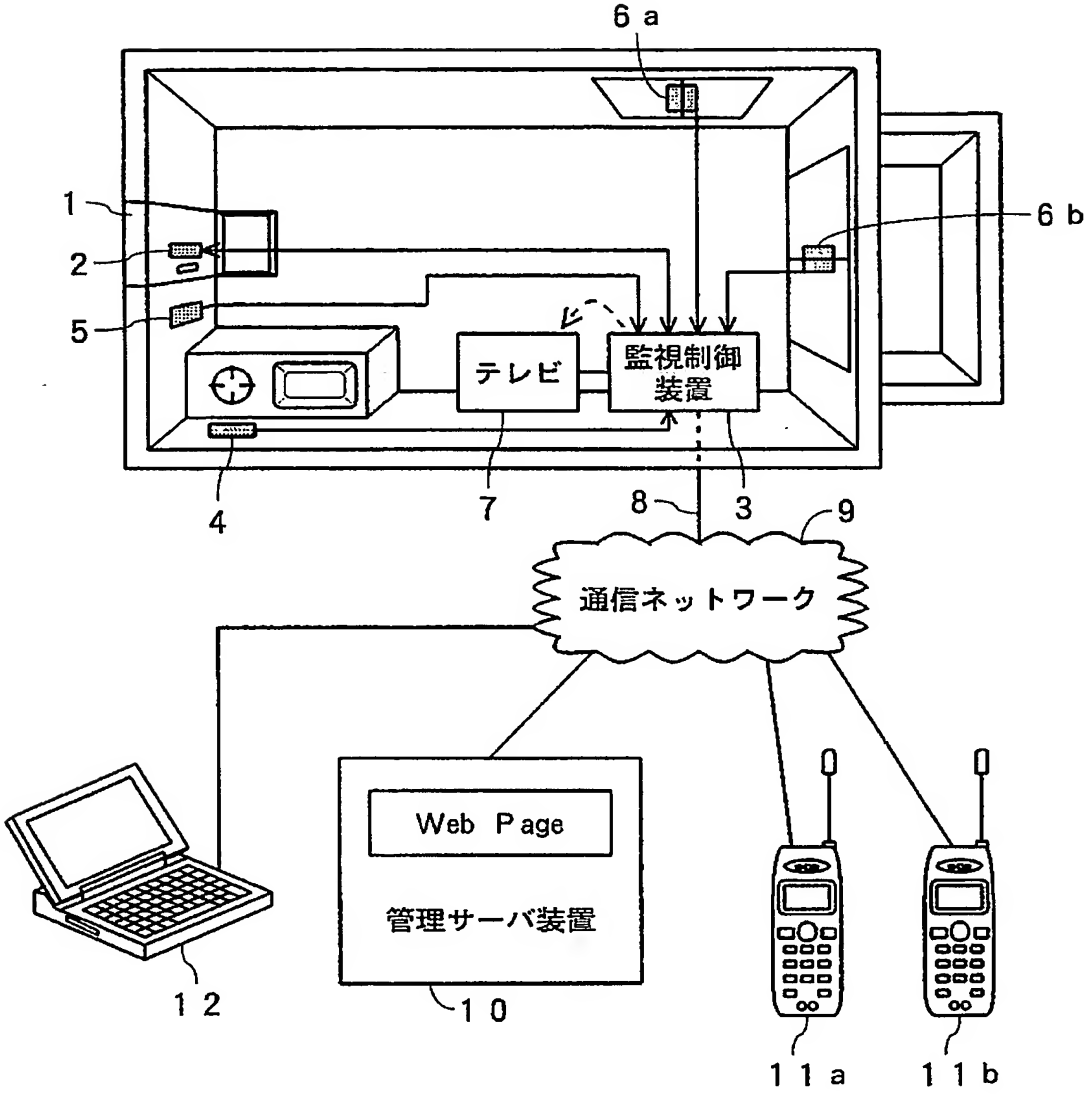
【図１】


１００１
ＩＣチップ
製造会社
１００１
ＩＣチップ
製造会社
一元管理された重複のないＩＣ製造番号付与
１００２
ＩＣチップ
１００２
ＩＣチップ
・・・・・
１００２
ＩＣチップ
１００３
ＩＣカード
（電子鍵カード）
製造工場
１００４
携帯電話端末
製造工場
１００５
ＰＤＡ
製造工場

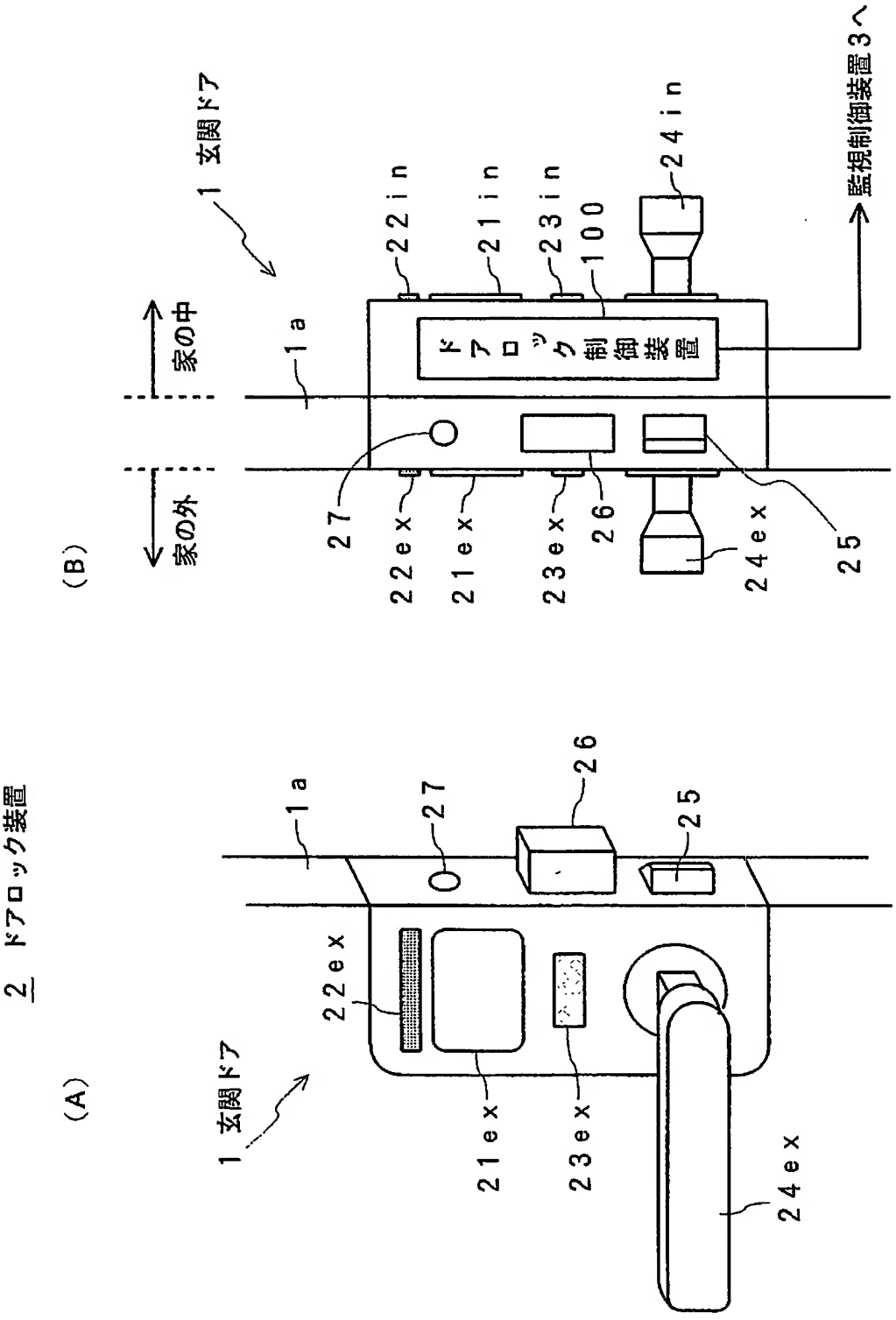
【図２】


００ＡＫＫ０００１
メーカー番号
カテゴリコード
シリアル番号

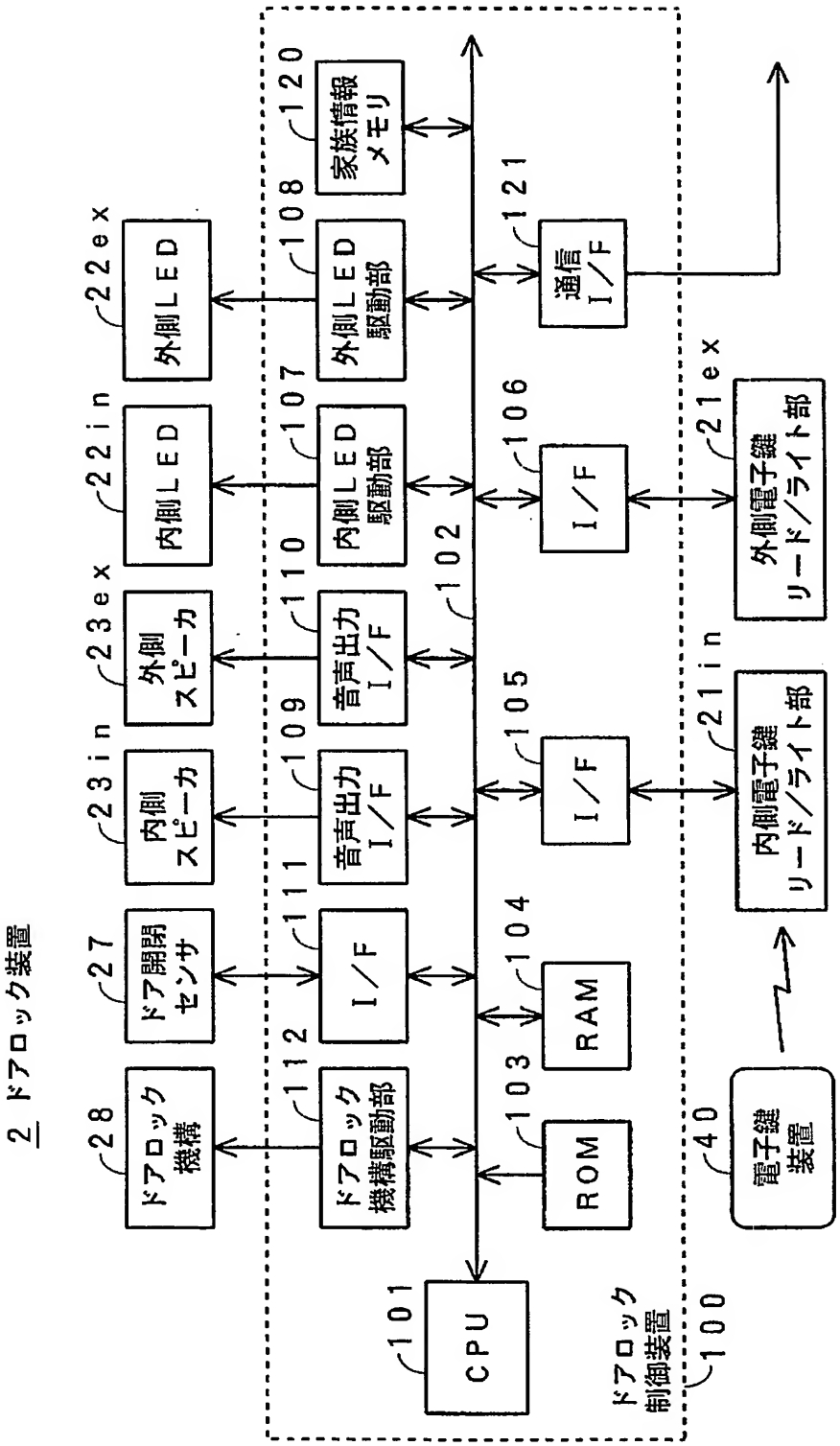
【図３】


6 a
1
2
5
6 b
テレビ
監視制御装置
4
7
8
3
9
通信ネットワーク
Web Page
管理サーバ装置
１２
１０
１１ａ
１１ｂ

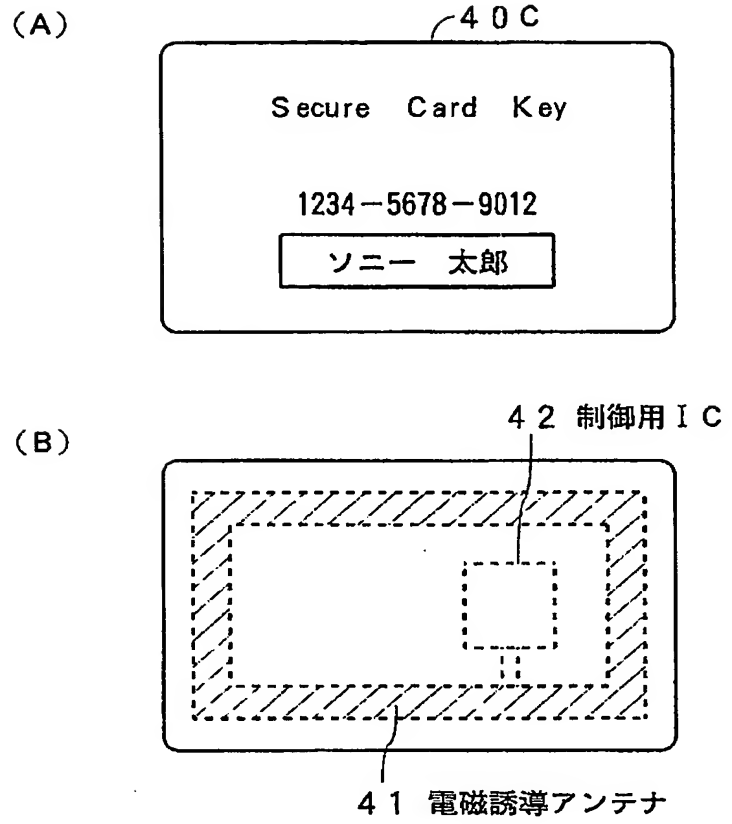
【図４】


(B)
1 玄関ドア
家の中
家の外
1a
22in
21in
23in
100
24in
ドアロック制御装置
監視制御装置3へ
27
22ex
21ex
23ex
26
24ex
25
2 ドアロック装置
(A)
1a
27
26
25
22ex
1 玄関ドア
21ex
23ex
24ex

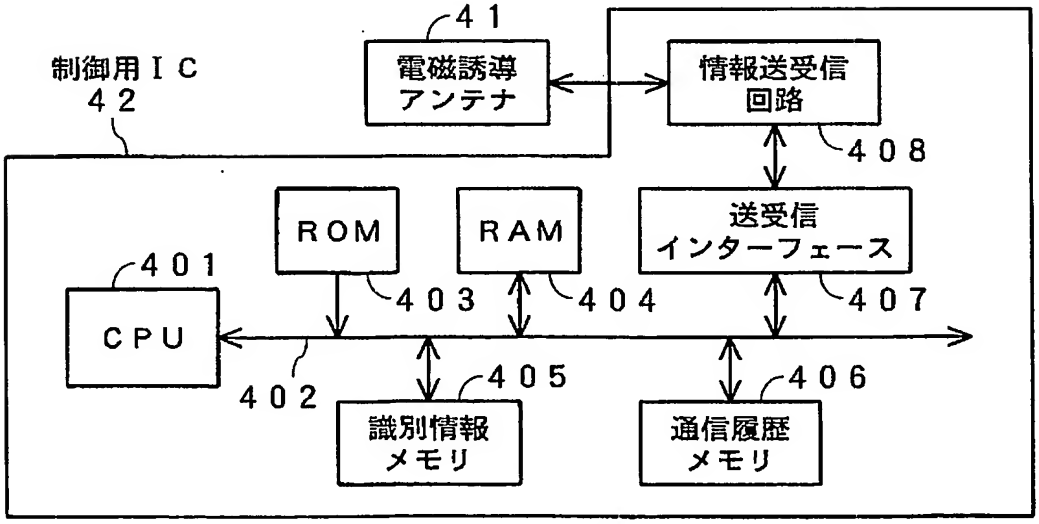
【図５】


2 ドアロック装置
ドアロック制御装置
100
CPU
101
ROM
103
RAM
104
I／F
105
I／F
106
I／F
111
I／F
112
ドアロック機構駆動部
107
内側LED駆動部
108
外側LED駆動部
109
音声出力I／F
110
音声出力I／F
121
通信I／F
120
家族情報メモリ
28
ドアロック機構
27
ドア開閉センサ
23in
内側スピーカ
23ex
外側スピーカ
22in
内側LED
22ex
外側LED
40
電子鍵装置
21in
内側電子鍵リード／ライト部
21ex
外側電子鍵リード／ライト部

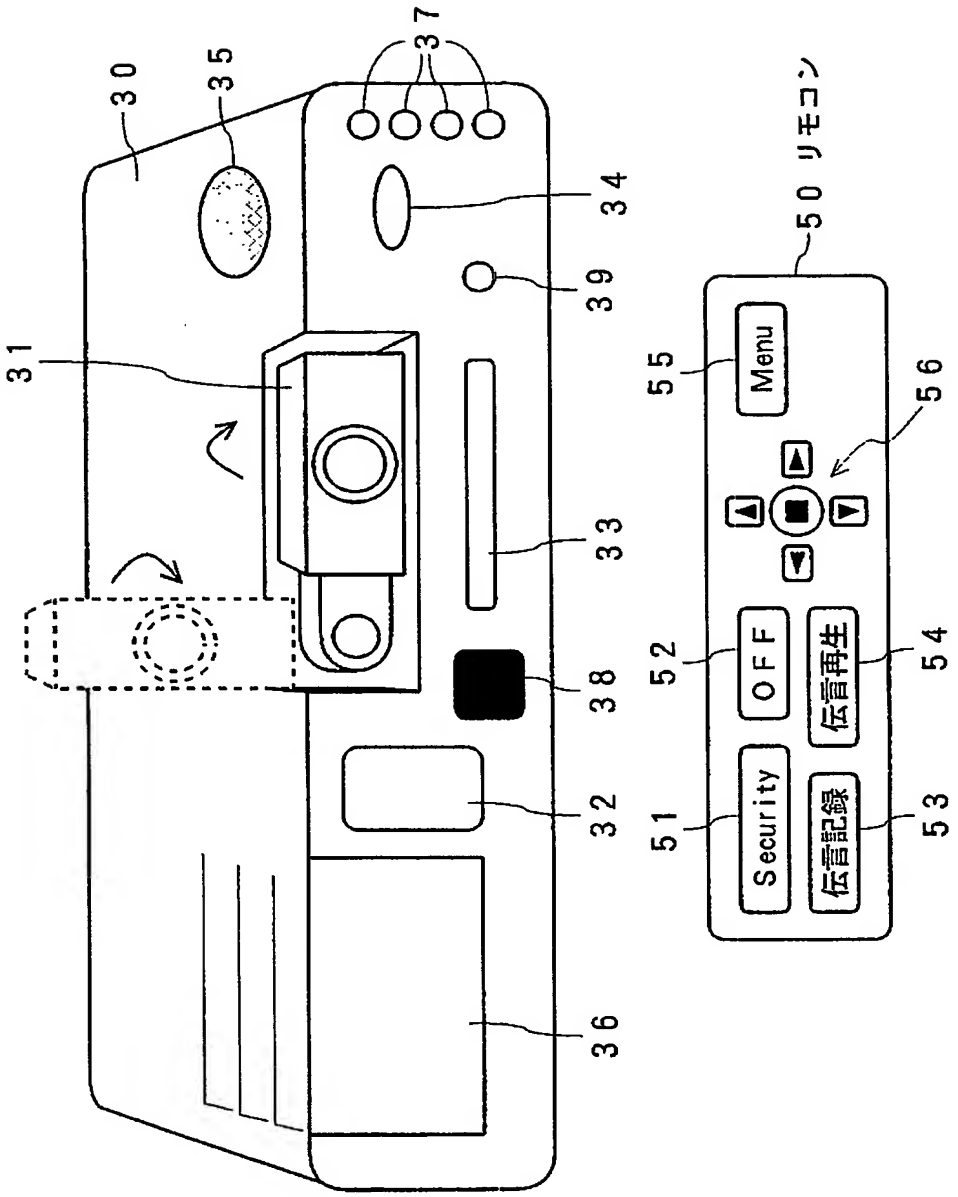
【図６】


（A）
４０Ｃ
Secure Card Key
1234－5678－9012
ソニー　太郎
（B）
４２ 制御用ＩＣ
４１ 電磁誘導アンテナ

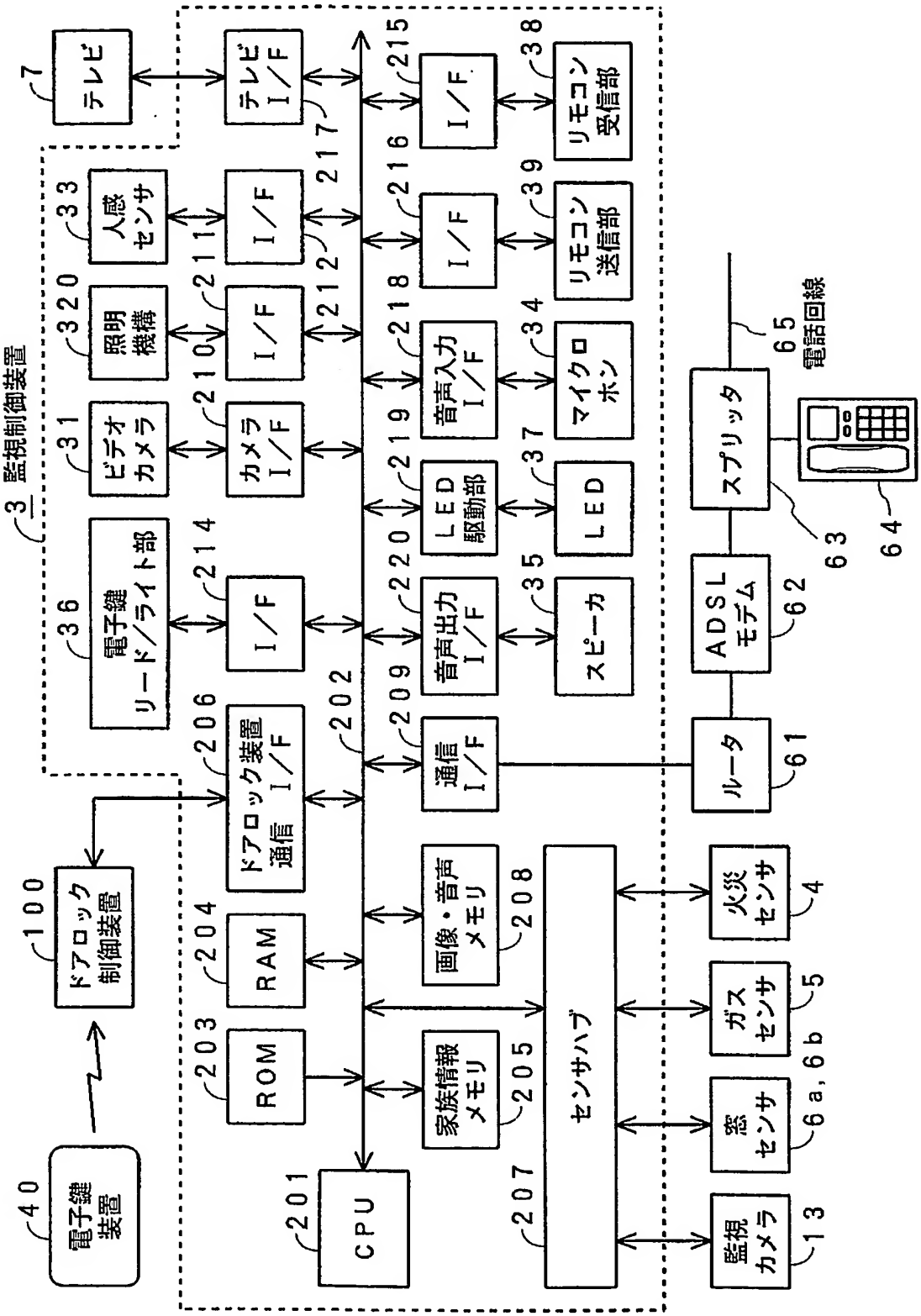
【図７】


４１
電磁誘導
アンテナ
制御用ＩＣ
４２
情報送受信
回路
４０８
ROM
RAM
送受信
インターフェース
４０１
CPU
４０３
４０４
４０７
４０２
４０５
４０６
識別情報
メモリ
通信履歴
メモリ

【図８】


３　監視制御装置
３０
３５
３７
３４
３９
３１
３３
３８
３２
３６
５０　リモコン
５５
Menu
５６
５２
ＯＦＦ
伝言再生
５４
５１
Security
伝言記録
５３

【図９】


3 監視制御装置
7 テレビ
テレビ I／F
215
I／F
38 リモコン 受信部
33 人感 センサ
211
I／F
216
I／F
39 リモコン 送信部
320 照明 機構
210
I／F
212
I／F
218
I／F
34 マイクロ ホン
31 ビデオ カメラ
カメラ I／F
217
219 音声入力 I／F
37 LED
LED 駆動部
214
220
35 スピーカ
音声出力 I／F
36 電子鍵 リード／ライト部
I／F
209
通信 I／F
206 ドアロック装置 通信 I／F
202
100 ドアロック 制御装置
204 RAM
208 画像・音声 メモリ
203 ROM
205 家族情報 メモリ
センサハブ
201 CPU
207
40 電子鍵 装置
火災 センサ
4
ガス センサ
5
窓 センサ
6a, 6b
監視 カメラ
13
ルータ
61
ADSL モデム
62
スプリッタ
63
64
65 電話回線

【図１０】

個人プロファイル情報

	識別情報 ・本鍵情報 ・バックアップ鍵情報	個人識別情報
	パスワード情報	個人情報
	氏名	
	住所	
	生年月日	
	年齢	
	続柄	
	登録日	
	銀行口座番号	
	電話番号	
	趣味／嗜好情報 ・好きなテレビ番組：ドラマ ・好きな音楽：ジャズ ・好きな映画：ＳＦ	
	入退出履歴情報	
	電子鍵登録・紛失履歴情報	

【図１１】

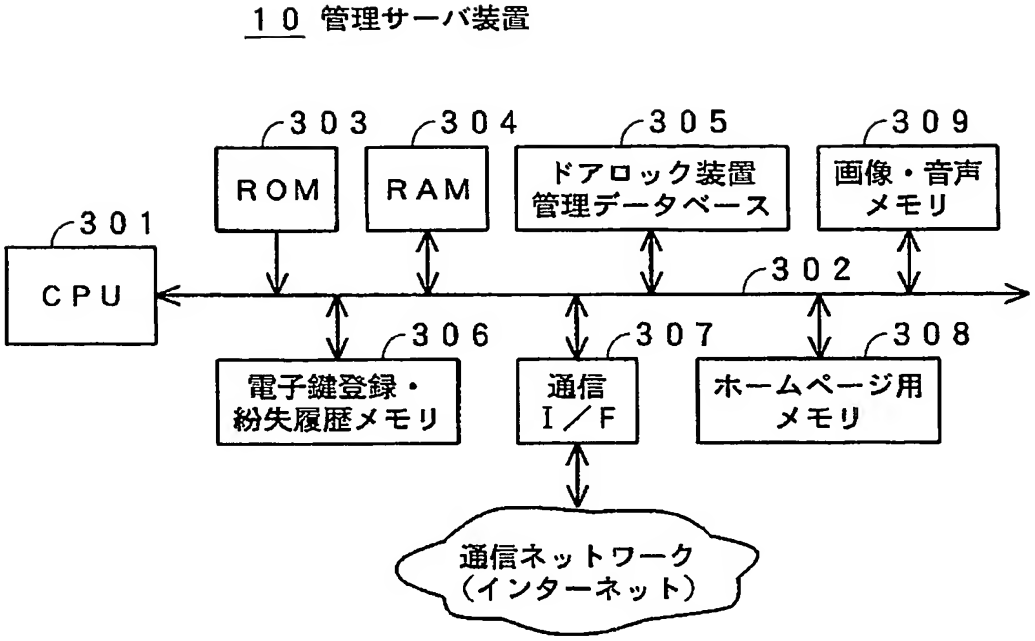
セキュリティレベル	父親	母親	子供
D	○	○	○
D	○	○	×
D	○	×	○
D	○	×	×
C	×	○	○
C	×	○	×
B	×	×	○
A	×	×	×

○：在宅
×：不在

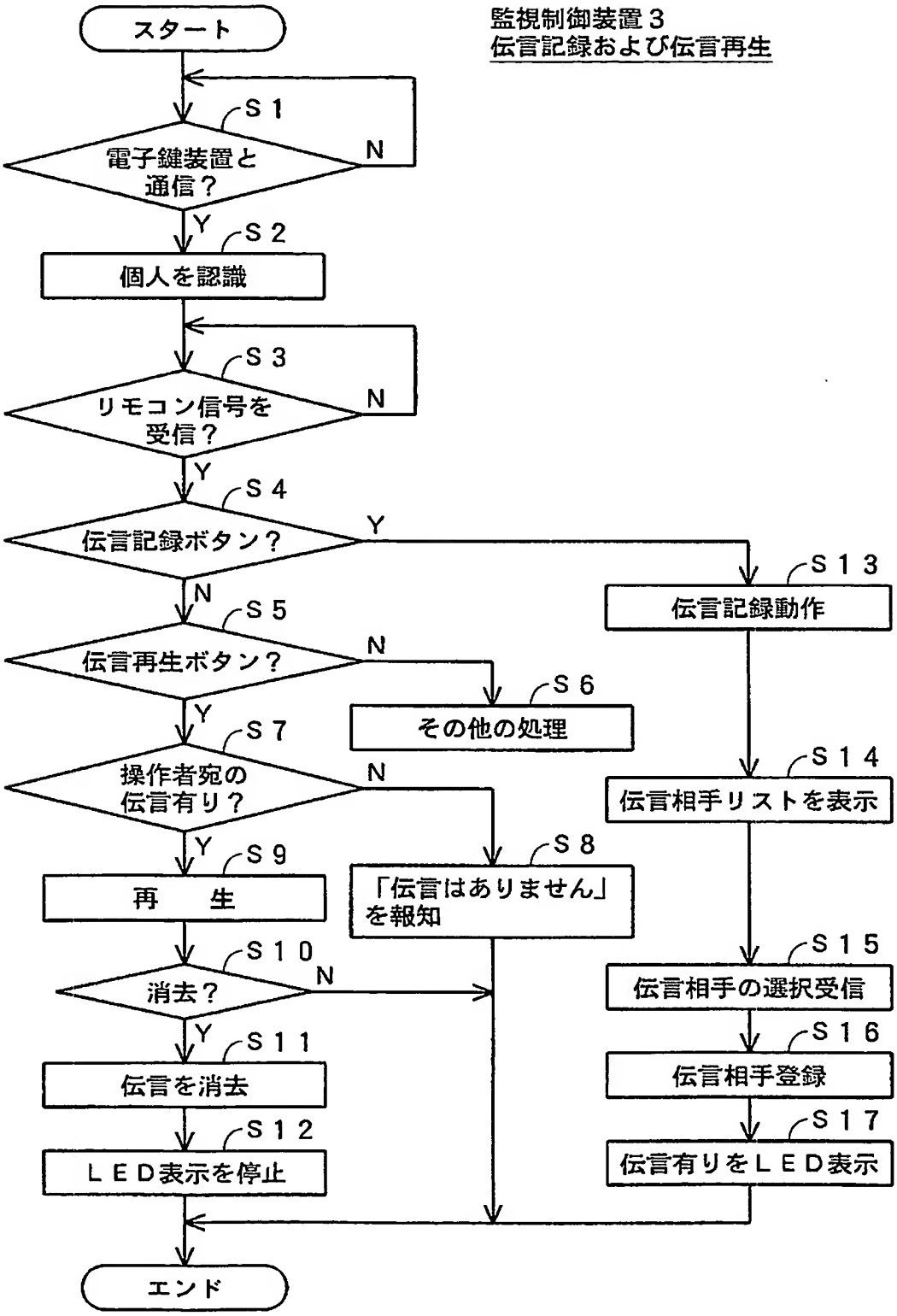
【図１２】

セキュリティレベル	窓・ドア監視	火災・ガス監視	カメラ監視
A	○	○	○
B	○	○	×
C	×	○	×
D	×	×	×

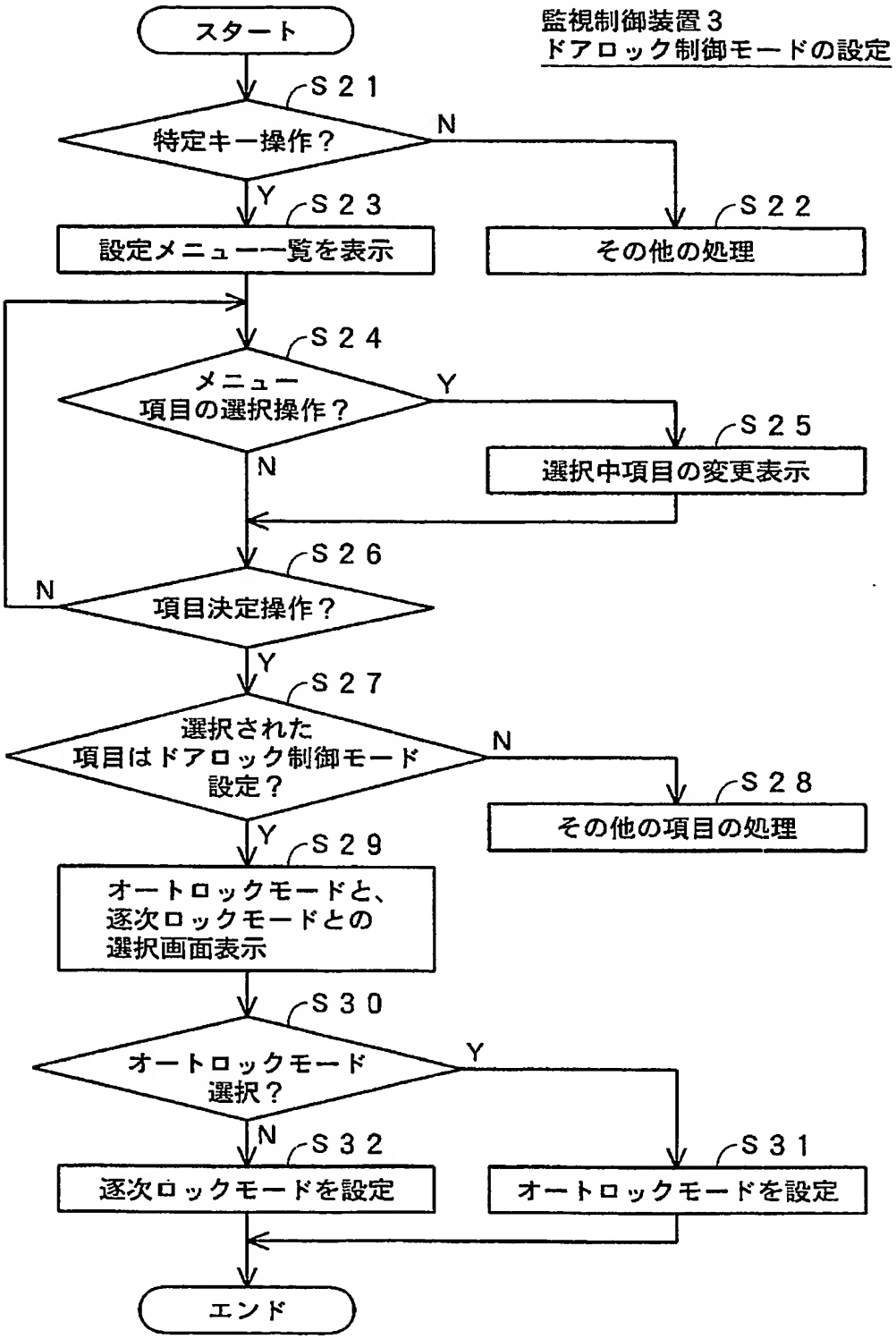
【図１３】


１０ 管理サーバ装置
３０３
３０４
３０５
３０９
ROM
RAM
ドアロック装置
管理データベース
画像・音声
メモリ
３０１
CPU
３０２
３０６
３０７
３０８
電子鍵登録・
紛失履歴メモリ
通信
Ｉ／Ｆ
ホームページ用
メモリ
通信ネットワーク
（インターネット）

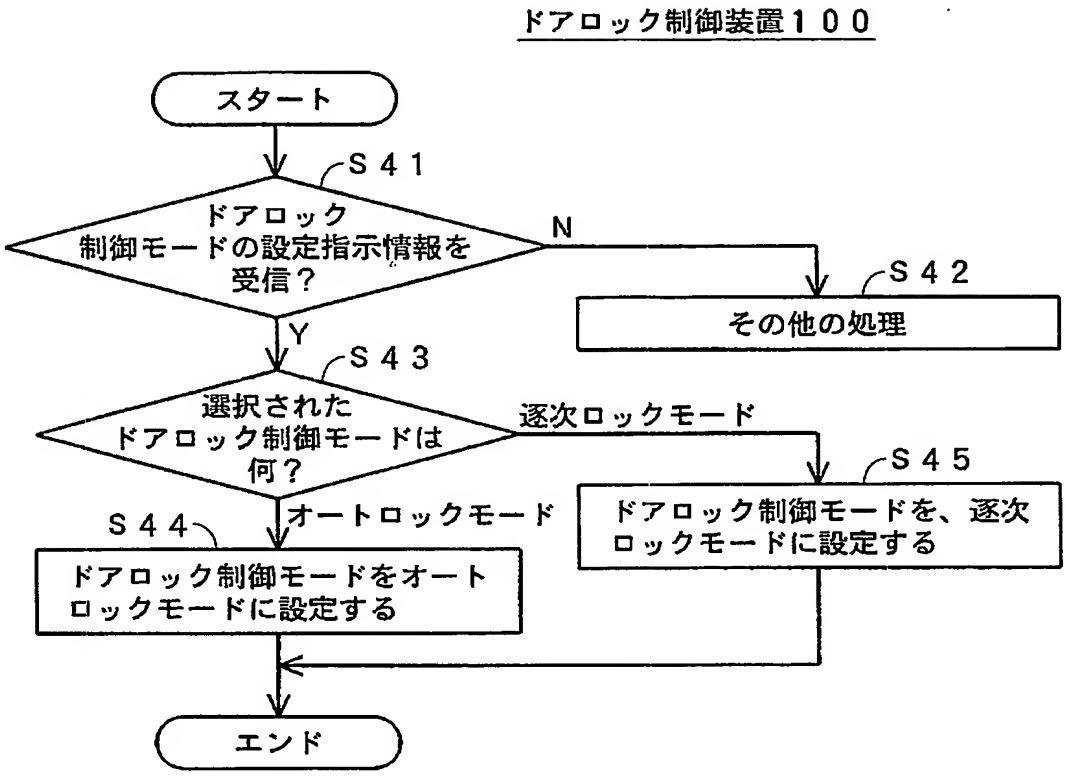
【図１４】


スタート
監視制御装置３
伝言記録および伝言再生
S１
電子鍵装置と通信？
N
Y
S２
個人を認識
S３
リモコン信号を受信？
N
Y
S４
伝言記録ボタン？
Y
N
S５
伝言再生ボタン？
N
Y
S６
その他の処理
S７
操作者宛の伝言有り？
N
Y
S８
「伝言はありません」を報知
S９
再　生
S１０
消去？
N
Y
S１１
伝言を消去
S１２
ＬＥＤ表示を停止
S１３
伝言記録動作
S１４
伝言相手リストを表示
S１５
伝言相手の選択受信
S１６
伝言相手登録
S１７
伝言有りをＬＥＤ表示
エンド

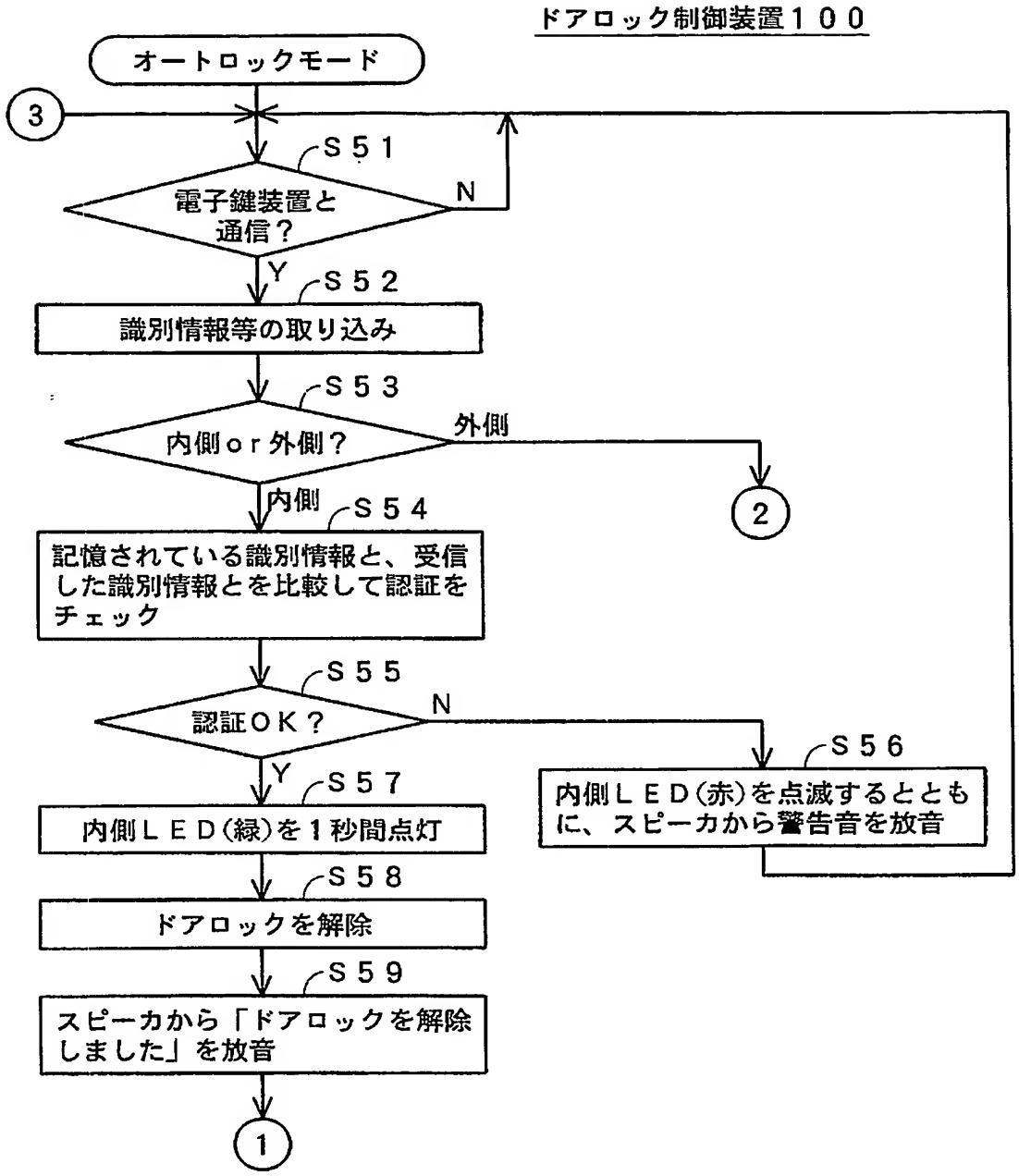
【図１５】


スタート
監視制御装置３
ドアロック制御モードの設定
Ｓ２１
特定キー操作？
N
Y
Ｓ２３
設定メニュー一覧を表示
Ｓ２２
その他の処理
Ｓ２４
メニュー
項目の選択操作？
Y
Ｓ２５
選択中項目の変更表示
N
Ｓ２６
項目決定操作？
N
Y
Ｓ２７
選択された
項目はドアロック制御モード
設定？
N
Ｓ２８
その他の項目の処理
Y
Ｓ２９
オートロックモードと、
逐次ロックモードとの
選択画面表示
Ｓ３０
オートロックモード
選択？
Y
N
Ｓ３２
逐次ロックモードを設定
Ｓ３１
オートロックモードを設定
エンド

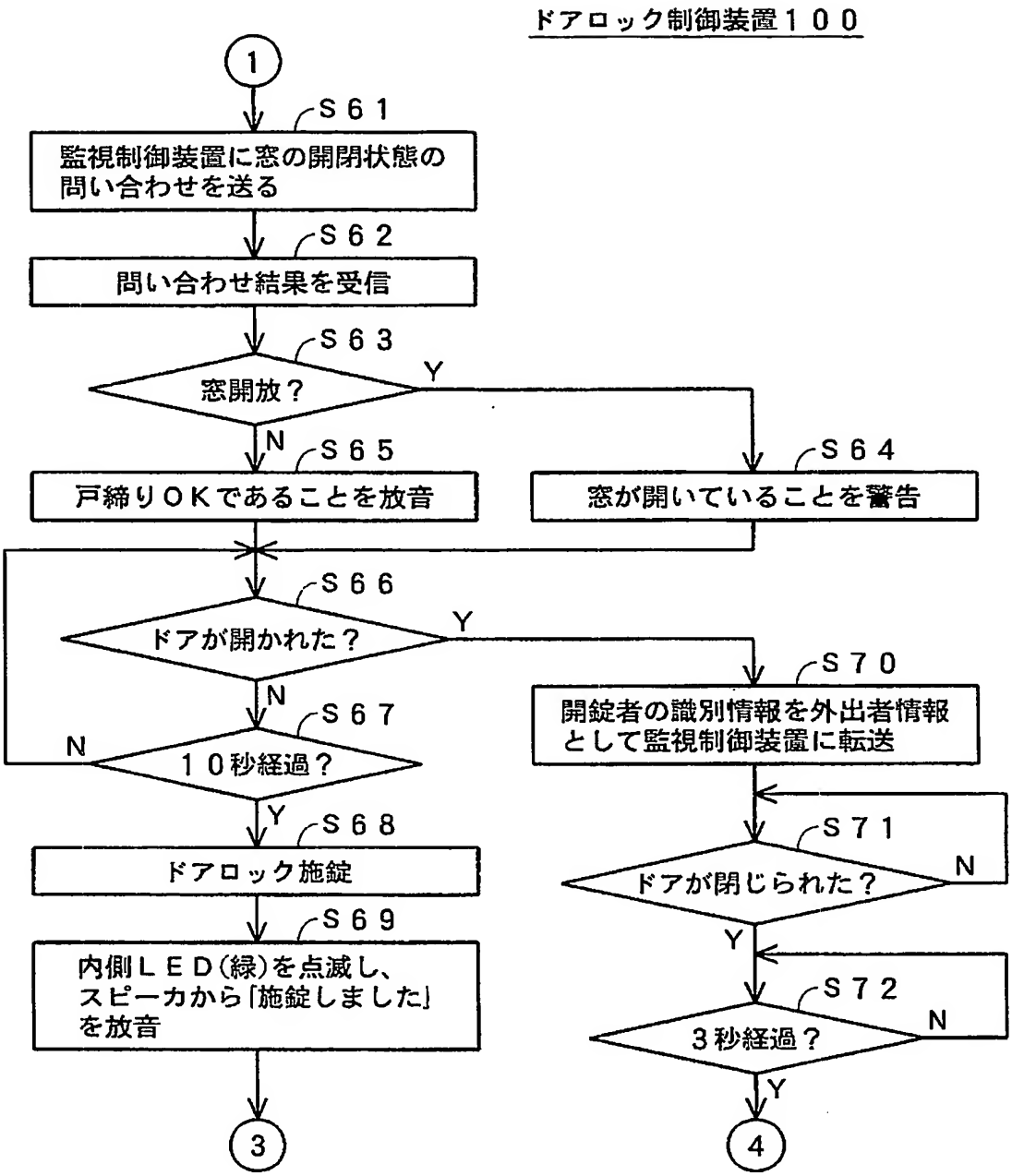
【図１６】


ドアロック制御装置１００
スタート
Ｓ４１
ドアロック制御モードの設定指示情報を受信？
N
Ｓ４２
その他の処理
Y
Ｓ４３
選択されたドアロック制御モードは何？
逐次ロックモード
Ｓ４５
ドアロック制御モードを、逐次ロックモードに設定する
オートロックモード
Ｓ４４
ドアロック制御モードをオートロックモードに設定する
エンド

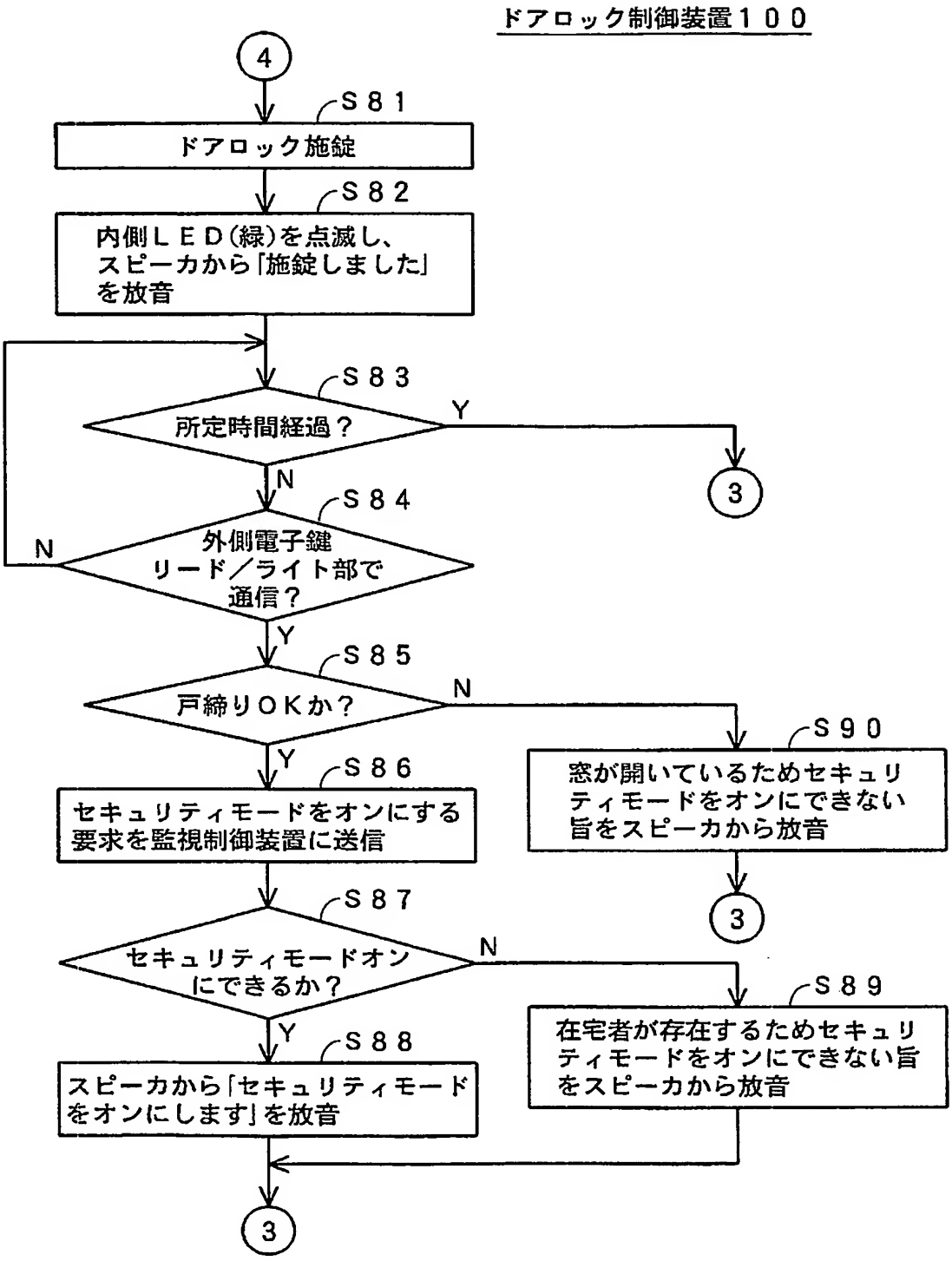
【図１７】


ドアロック制御装置１００
オートロックモード
3
S５１
電子鍵装置と通信？
N
Y
S５２
識別情報等の取り込み
S５３
内側ｏｒ外側？
外側
2
内側
S５４
記憶されている識別情報と、受信した識別情報とを比較して認証をチェック
S５５
認証ＯＫ？
N
S５６
内側ＬＥＤ(赤)を点滅するとともに、スピーカから警告音を放音
Y
S５７
内側ＬＥＤ(緑)を１秒間点灯
S５８
ドアロックを解除
S５９
スピーカから「ドアロックを解除しました」を放音
1

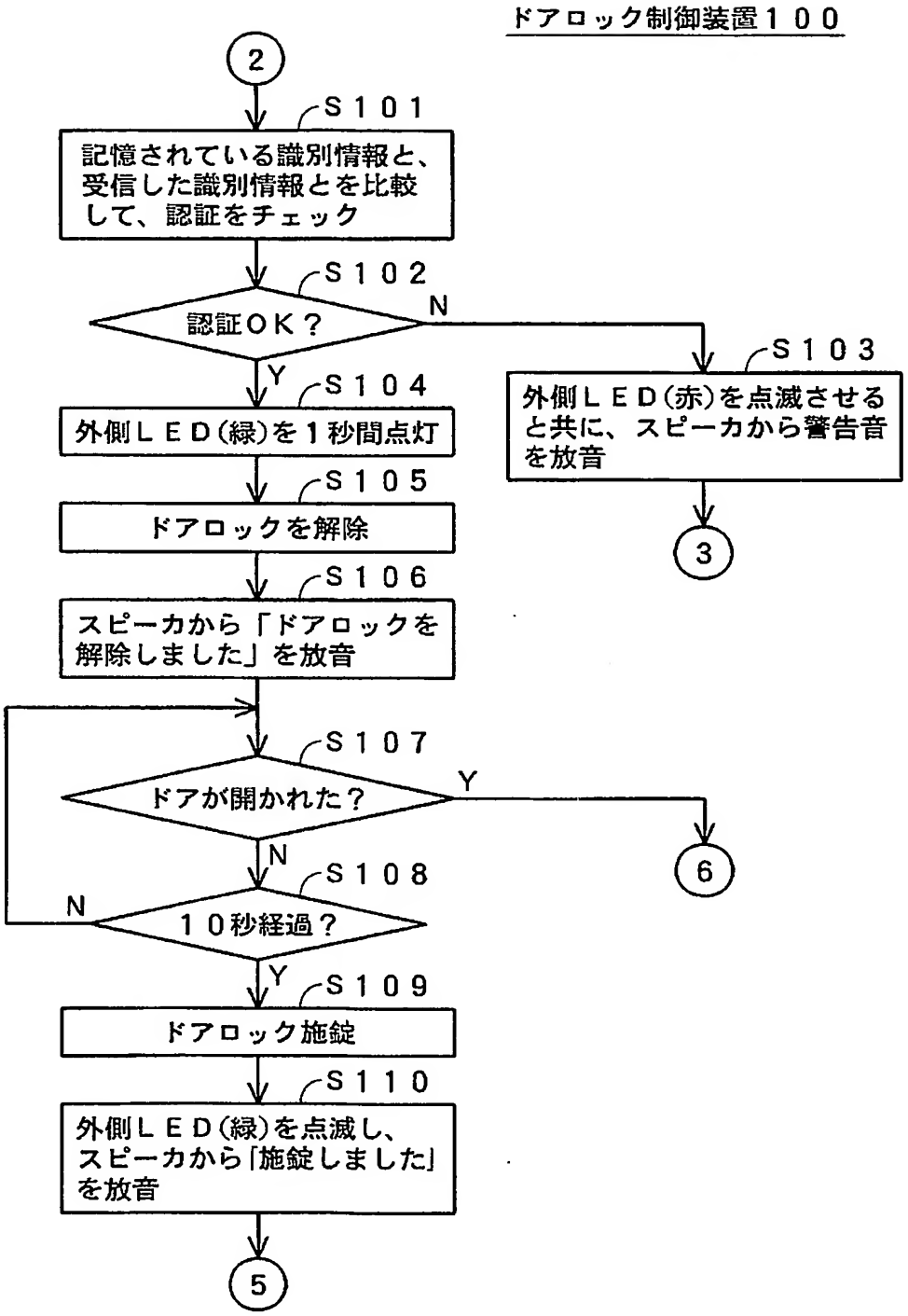
【図１８】


ドアロック制御装置１００
1
S６１
監視制御装置に窓の開閉状態の問い合わせを送る
S６２
問い合わせ結果を受信
S６３
窓開放？
Y
N
S６５
戸締りＯＫであることを放音
S６４
窓が開いていることを警告
S６６
ドアが開かれた？
Y
N
S６７
１０秒経過？
N
Y
S６８
ドアロック施錠
S６９
内側ＬＥＤ(緑)を点滅し、スピーカから「施錠しました」を放音
3
S７０
開錠者の識別情報を外出者情報として監視制御装置に転送
S７１
ドアが閉じられた？
N
Y
S７２
３秒経過？
N
Y
4

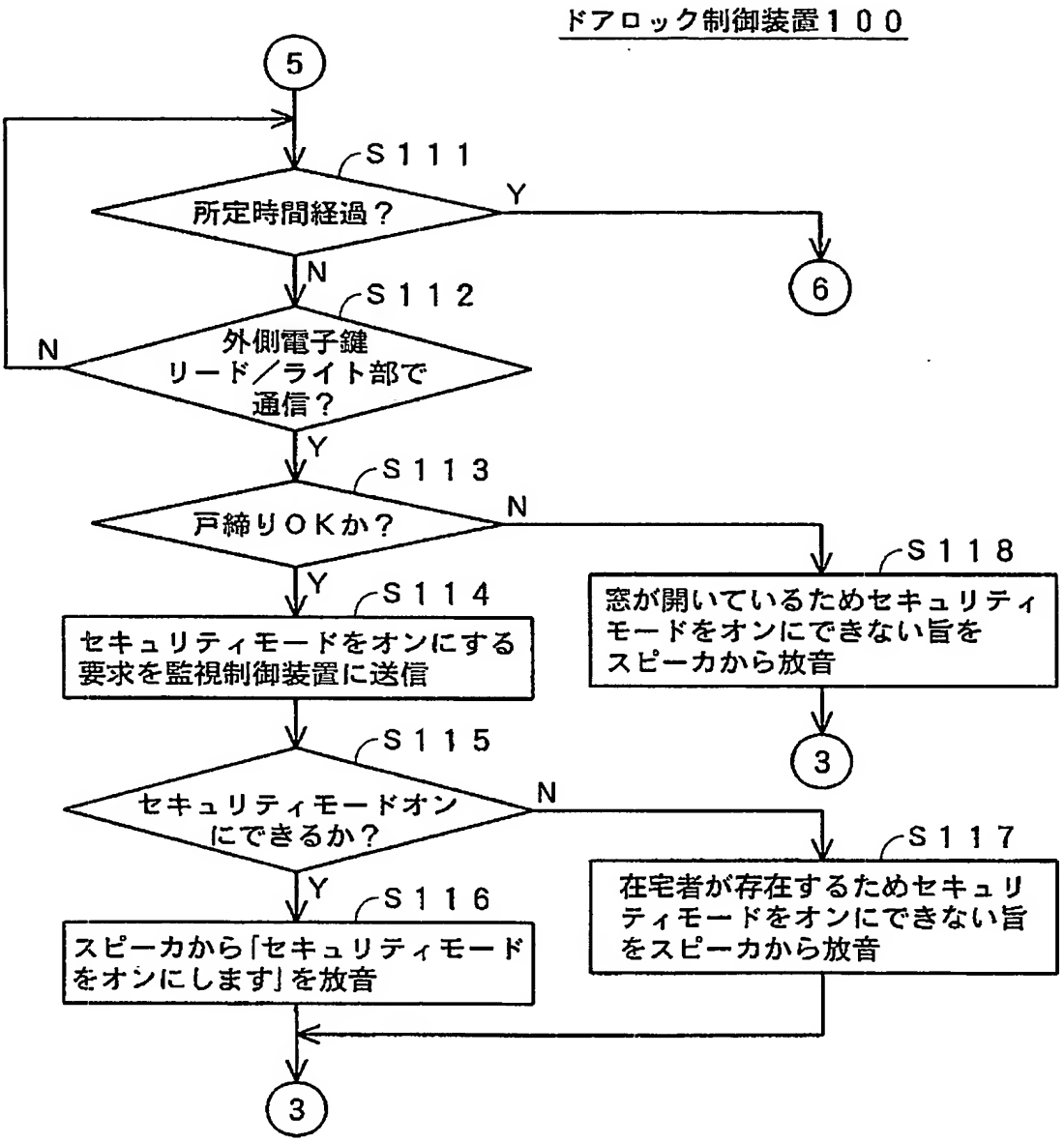
【図１９】


ドアロック制御装置１００
4
S81
ドアロック施錠
S82
内側ＬＥＤ(緑)を点滅し、スピーカから「施錠しました」を放音
S83
所定時間経過？
Y
N
3
S84
外側電子鍵リード／ライト部で通信？
N
Y
S85
戸締りＯＫか？
N
Y
S90
窓が開いているためセキュリティモードをオンにできない旨をスピーカから放音
3
S86
セキュリティモードをオンにする要求を監視制御装置に送信
S87
セキュリティモードオンにできるか？
N
Y
S89
在宅者が存在するためセキュリティモードをオンにできない旨をスピーカから放音
S88
スピーカから「セキュリティモードをオンにします」を放音
3

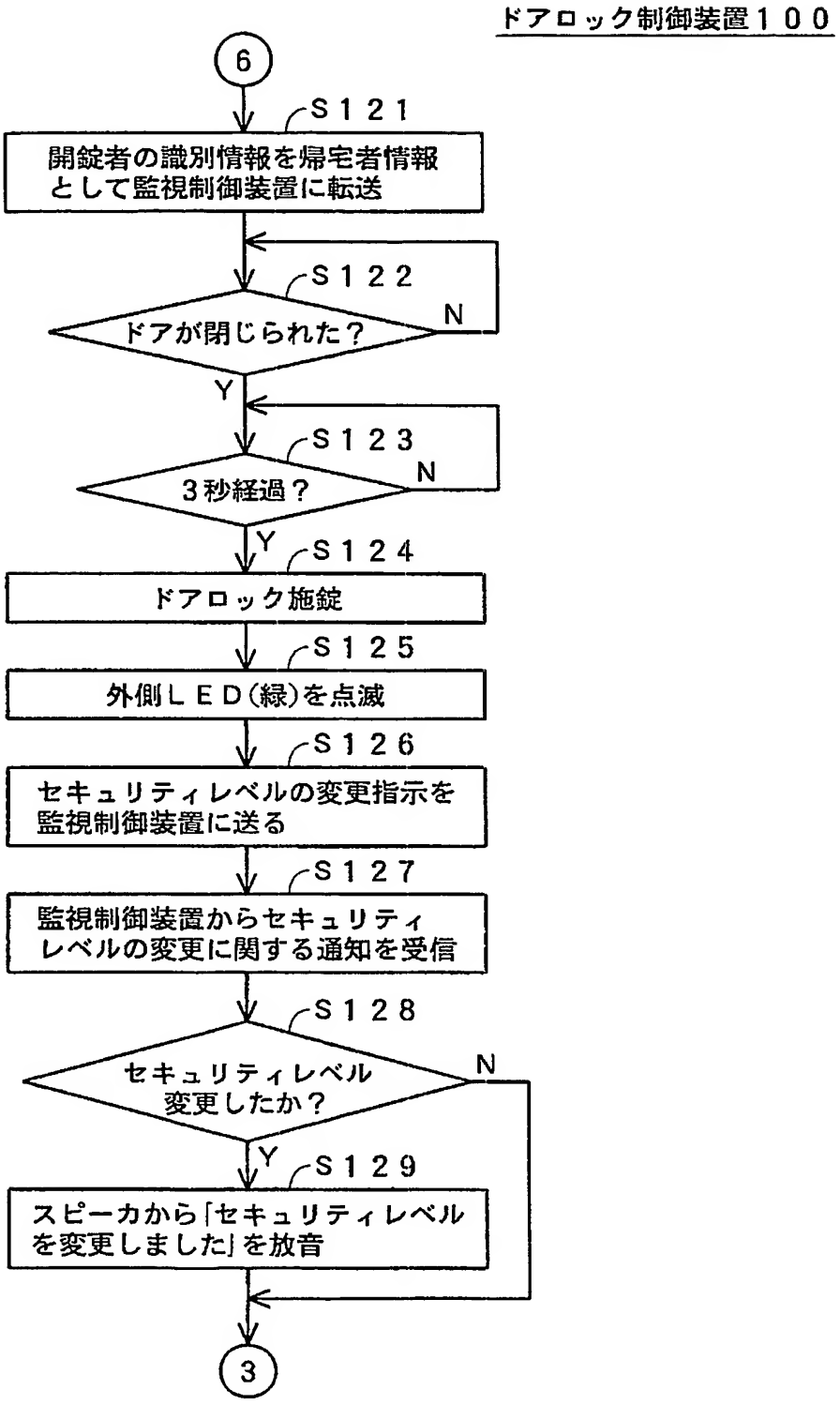
【図２０】


ドアロック制御装置１００
2
S１０１
記憶されている識別情報と、受信した識別情報とを比較して、認証をチェック
S１０２
認証ＯＫ？
N
S１０３
外側ＬＥＤ(赤)を点滅させると共に、スピーカから警告音を放音
3
Y
S１０４
外側ＬＥＤ(緑)を１秒間点灯
S１０５
ドアロックを解除
S１０６
スピーカから「ドアロックを解除しました」を放音
S１０７
ドアが開かれた？
Y
6
N
S１０８
１０秒経過？
N
Y
S１０９
ドアロック施錠
S１１０
外側ＬＥＤ(緑)を点滅し、スピーカから「施錠しました」を放音
5

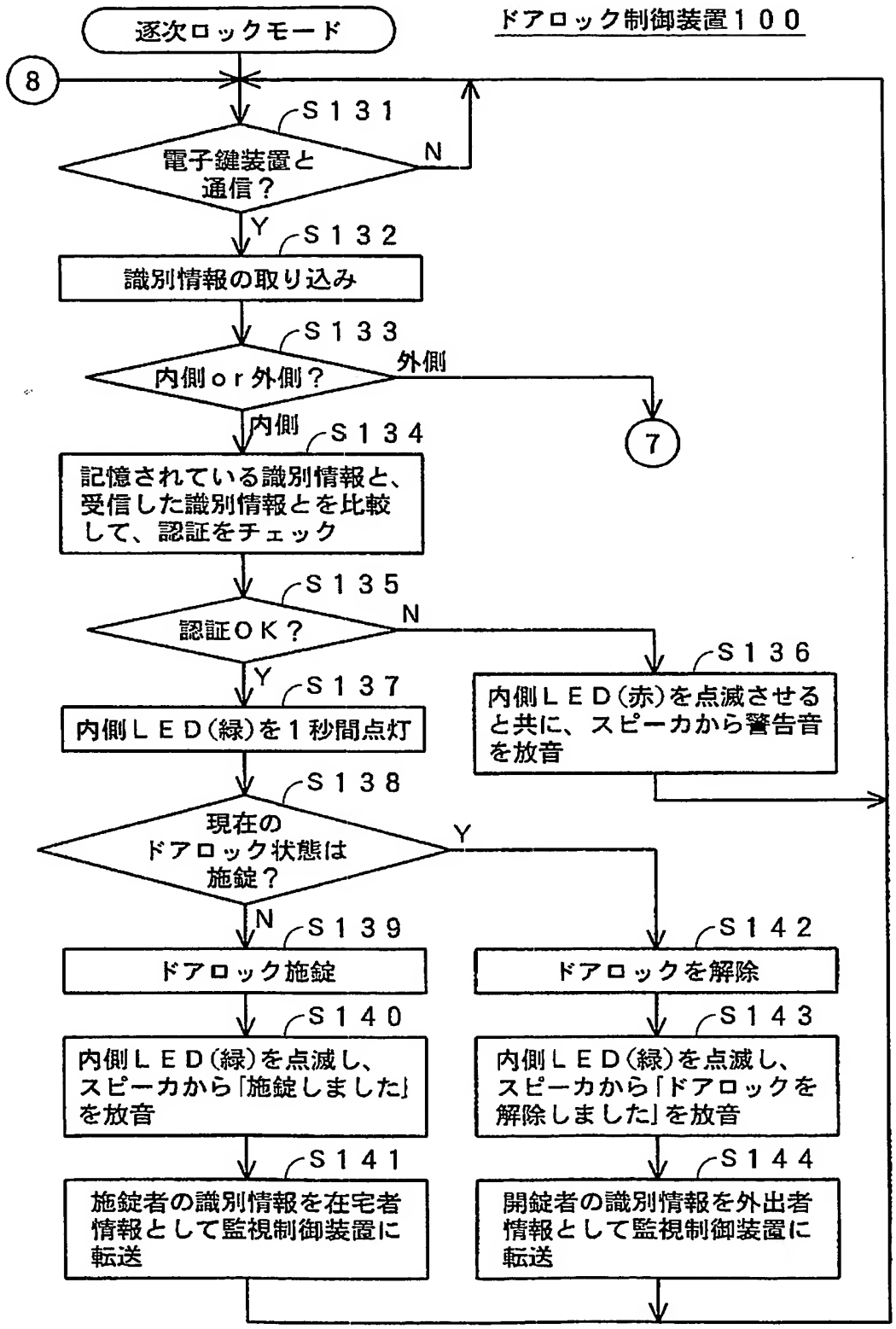
【図２１】


ドアロック制御装置１００
5
S１１１
所定時間経過？
Y
6
N
S１１２
外側電子鍵
リード／ライト部で
通信？
N
Y
S１１３
戸締りＯＫか？
N
Y
S１１４
セキュリティモードをオンにする
要求を監視制御装置に送信
S１１５
セキュリティモードオン
にできるか？
N
Y
S１１６
スピーカから「セキュリティモード
をオンにします」を放音
S１１８
窓が開いているためセキュリティ
モードをオンにできない旨を
スピーカから放音
3
S１１７
在宅者が存在するためセキュリ
ティモードをオンにできない旨
をスピーカから放音
3

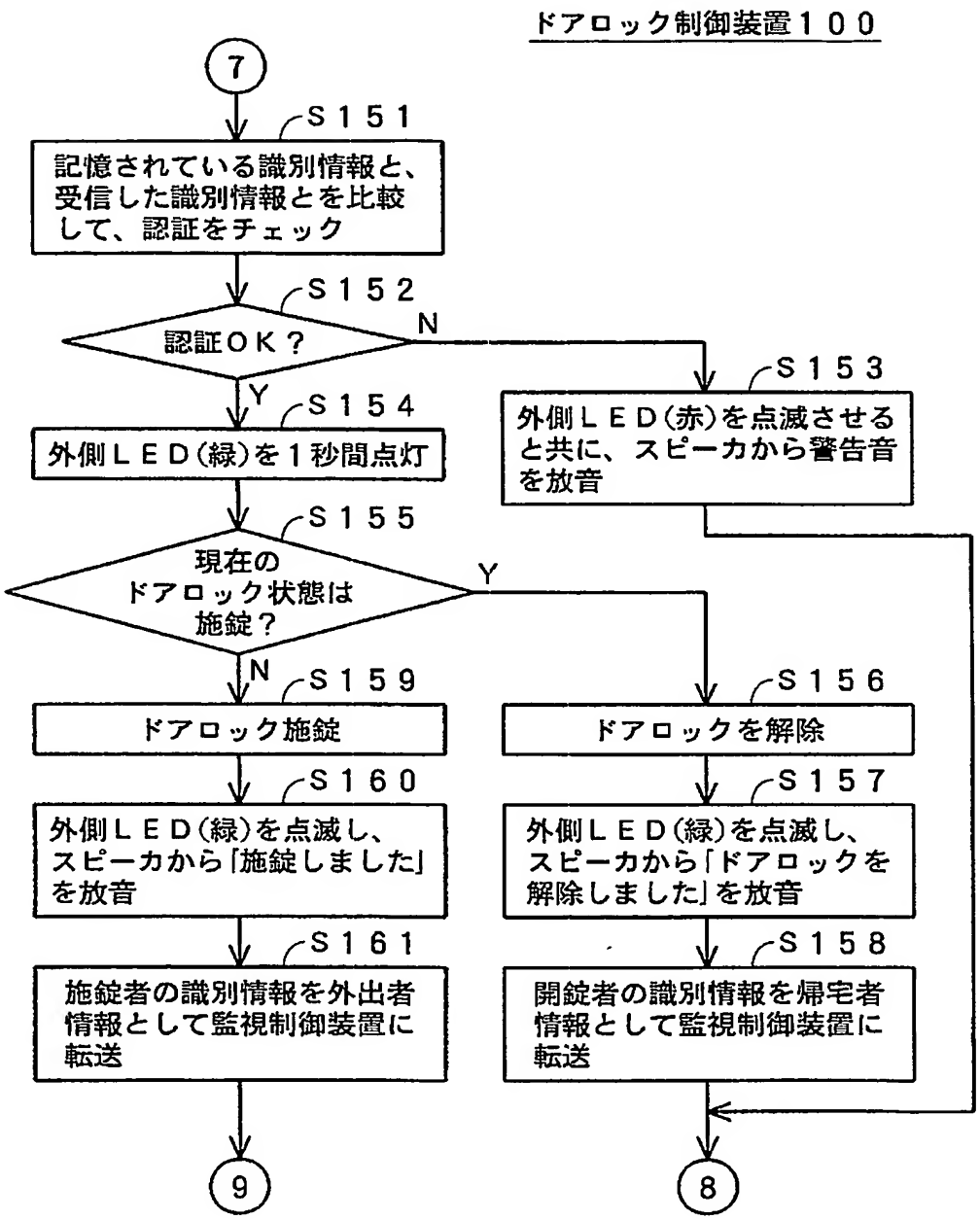
【図２２】


ドアロック制御装置１００
6
S１２１
開錠者の識別情報を帰宅者情報として監視制御装置に転送
S１２２
ドアが閉じられた？
N
Y
S１２３
３秒経過？
N
Y
S１２４
ドアロック施錠
S１２５
外側ＬＥＤ(緑)を点滅
S１２６
セキュリティレベルの変更指示を監視制御装置に送る
S１２７
監視制御装置からセキュリティレベルの変更に関する通知を受信
S１２８
セキュリティレベル変更したか？
N
Y
S１２９
スピーカから「セキュリティレベルを変更しました」を放音
3

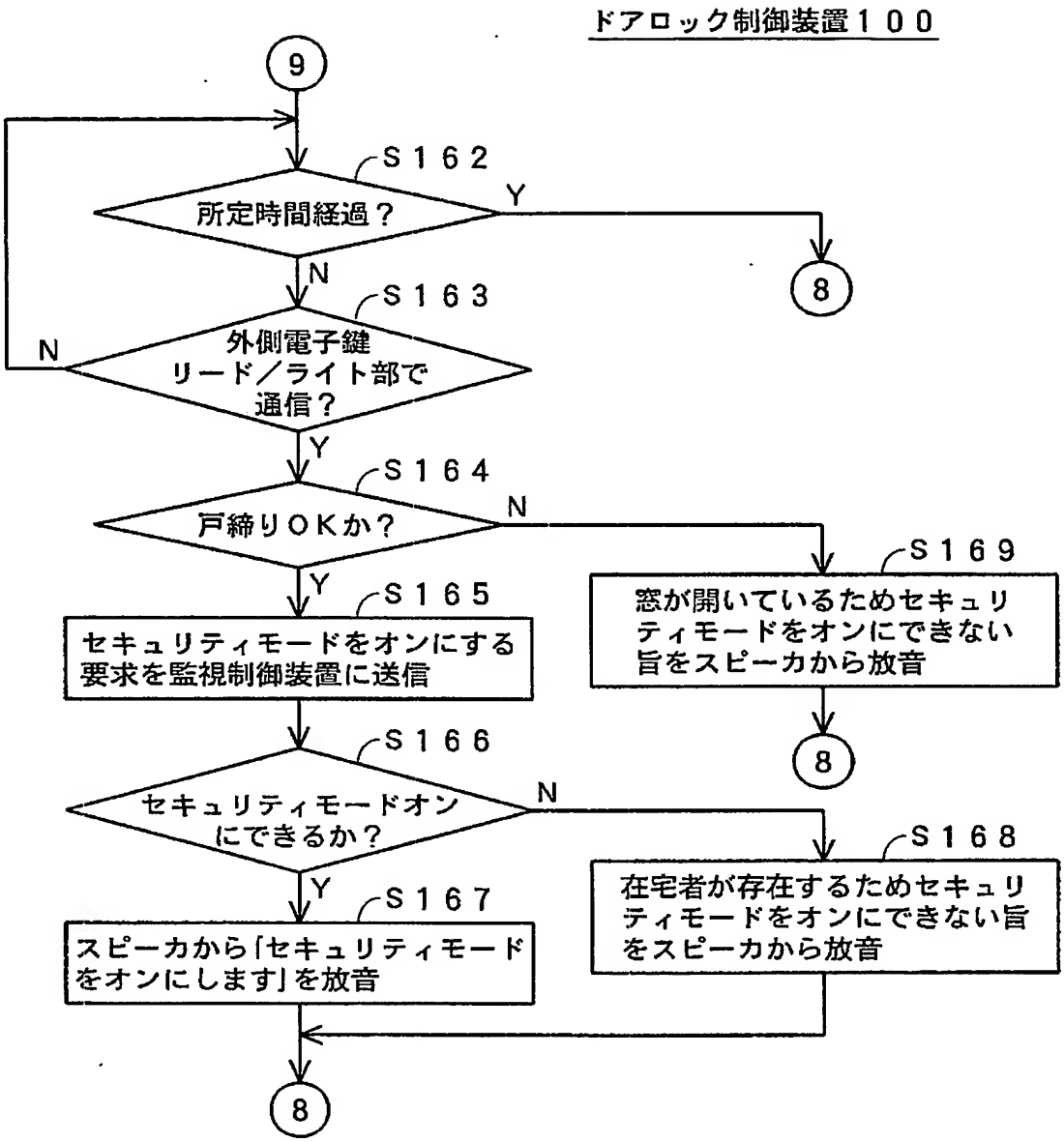
【図２３】


逐次ロックモード
ドアロック制御装置１００
8
S１３１
電子鍵装置と通信？
N
Y
S１３２
識別情報の取り込み
S１３３
内側ｏｒ外側？
外側
内側
7
S１３４
記憶されている識別情報と、受信した識別情報とを比較して、認証をチェック
S１３５
認証ＯＫ？
N
Y
S１３６
内側ＬＥＤ(赤)を点滅させると共に、スピーカから警告音を放音
S１３７
内側ＬＥＤ(緑)を１秒間点灯
S１３８
現在のドアロック状態は施錠？
Y
N
S１３９
ドアロック施錠
S１４０
内側ＬＥＤ(緑)を点滅し、スピーカから「施錠しました」を放音
S１４１
施錠者の識別情報を在宅者情報として監視制御装置に転送
S１４２
ドアロックを解除
S１４３
内側ＬＥＤ(緑)を点滅し、スピーカから「ドアロックを解除しました」を放音
S１４４
開錠者の識別情報を外出者情報として監視制御装置に転送

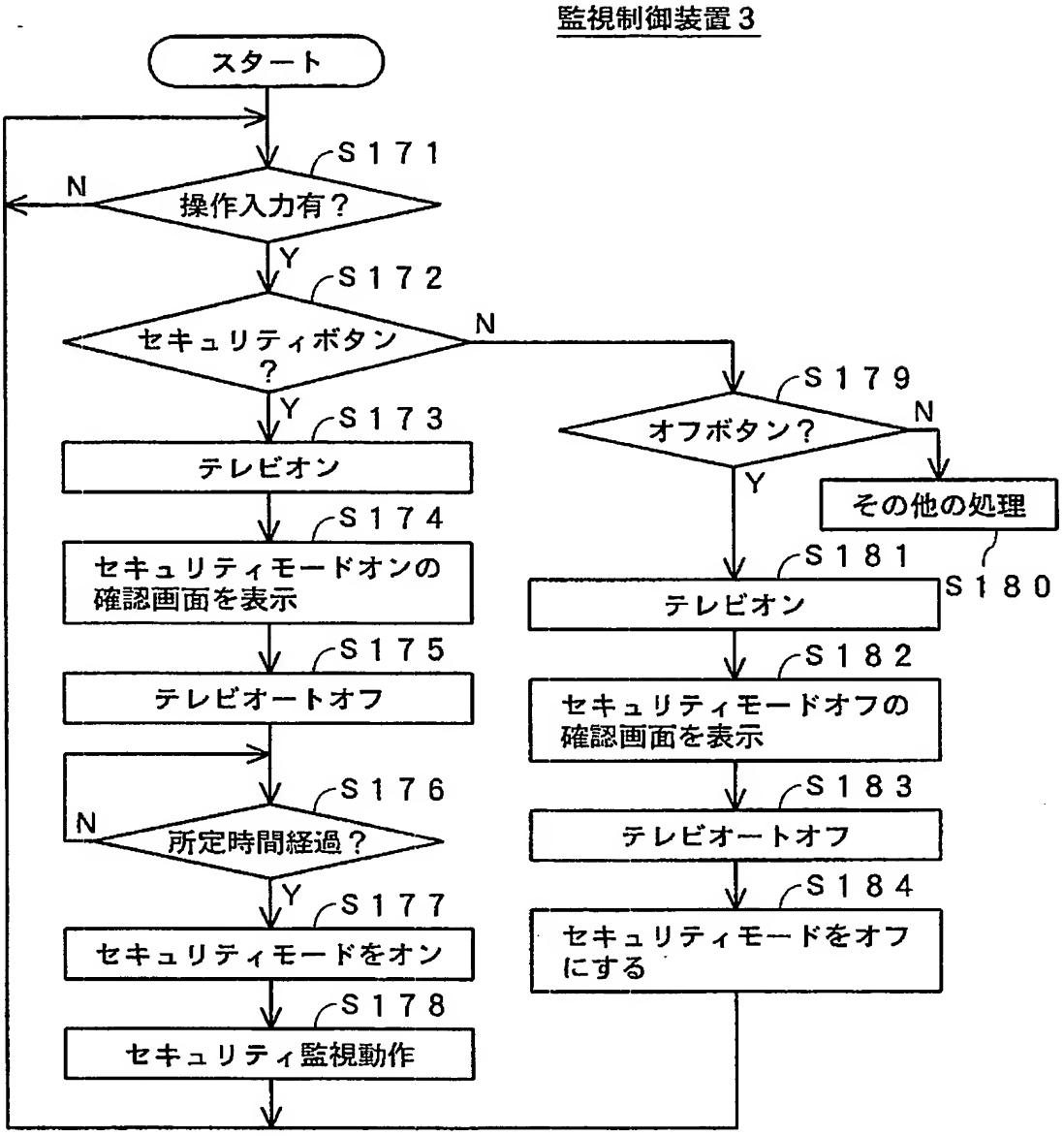
【図２４】


ドアロック制御装置１００
7
S１５１
記憶されている識別情報と、受信した識別情報とを比較して、認証をチェック
S１５２
認証ＯＫ？
N
Y
S１５３
外側ＬＥＤ(赤)を点滅させると共に、スピーカから警告音を放音
S１５４
外側ＬＥＤ(緑)を１秒間点灯
S１５５
現在のドアロック状態は施錠？
Y
N
S１５９
ドアロック施錠
S１６０
外側ＬＥＤ(緑)を点滅し、スピーカから「施錠しました」を放音
S１６１
施錠者の識別情報を外出者情報として監視制御装置に転送
9
S１５６
ドアロックを解除
S１５７
外側ＬＥＤ(緑)を点滅し、スピーカから「ドアロックを解除しました」を放音
S１５８
開錠者の識別情報を帰宅者情報として監視制御装置に転送
8

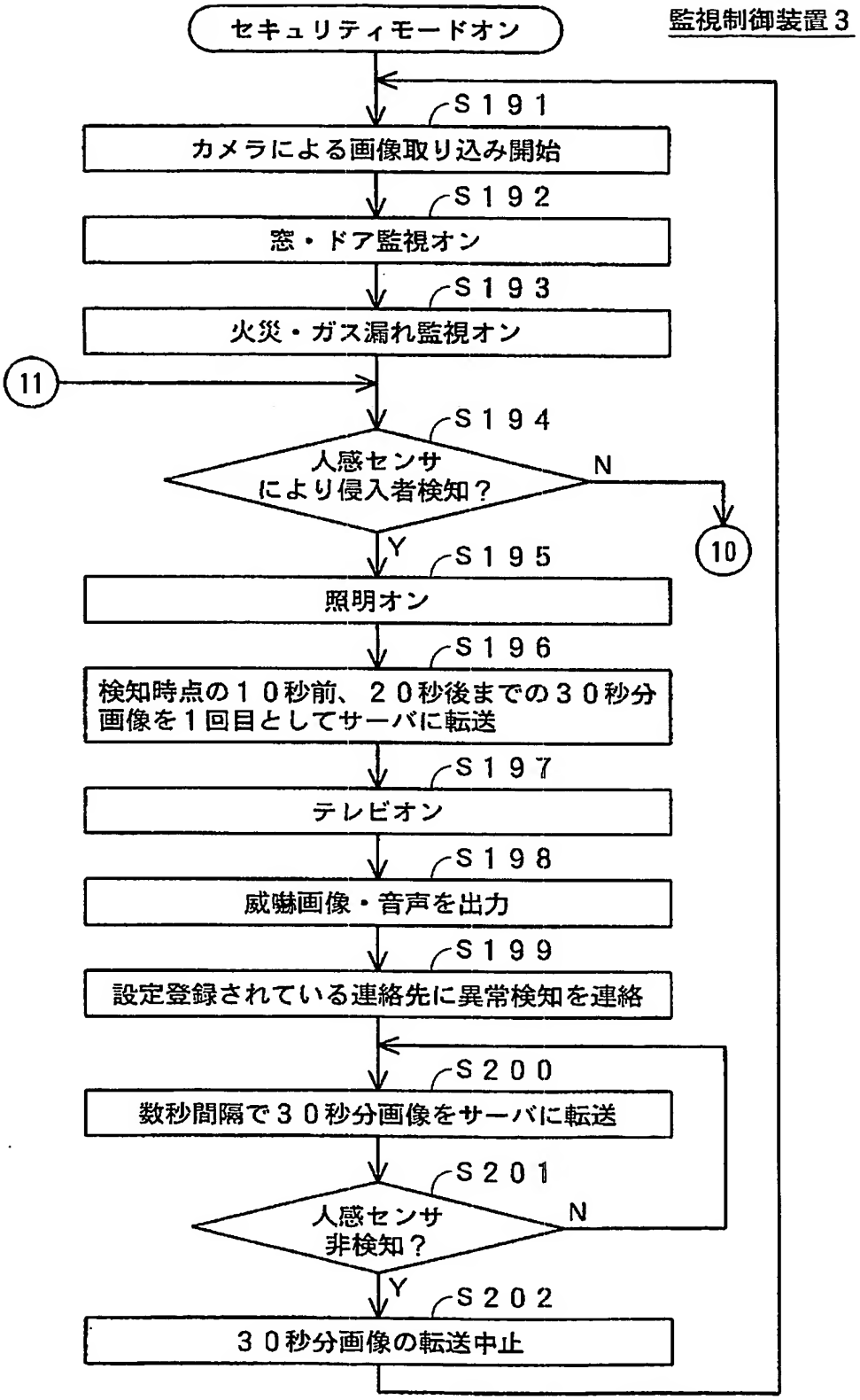
【図２５】


ドアロック制御装置１００
9
S１６２
所定時間経過？
Y
N
8
S１６３
外側電子鍵
リード／ライト部で
通信？
N
Y
S１６４
戸締りＯＫか？
N
Y
S１６９
窓が開いているためセキュリティモードをオンにできない旨をスピーカから放音
8
S１６５
セキュリティモードをオンにする要求を監視制御装置に送信
S１６６
セキュリティモードオンにできるか？
N
Y
S１６８
在宅者が存在するためセキュリティモードをオンにできない旨をスピーカから放音
S１６７
スピーカから「セキュリティモードをオンにします」を放音
8

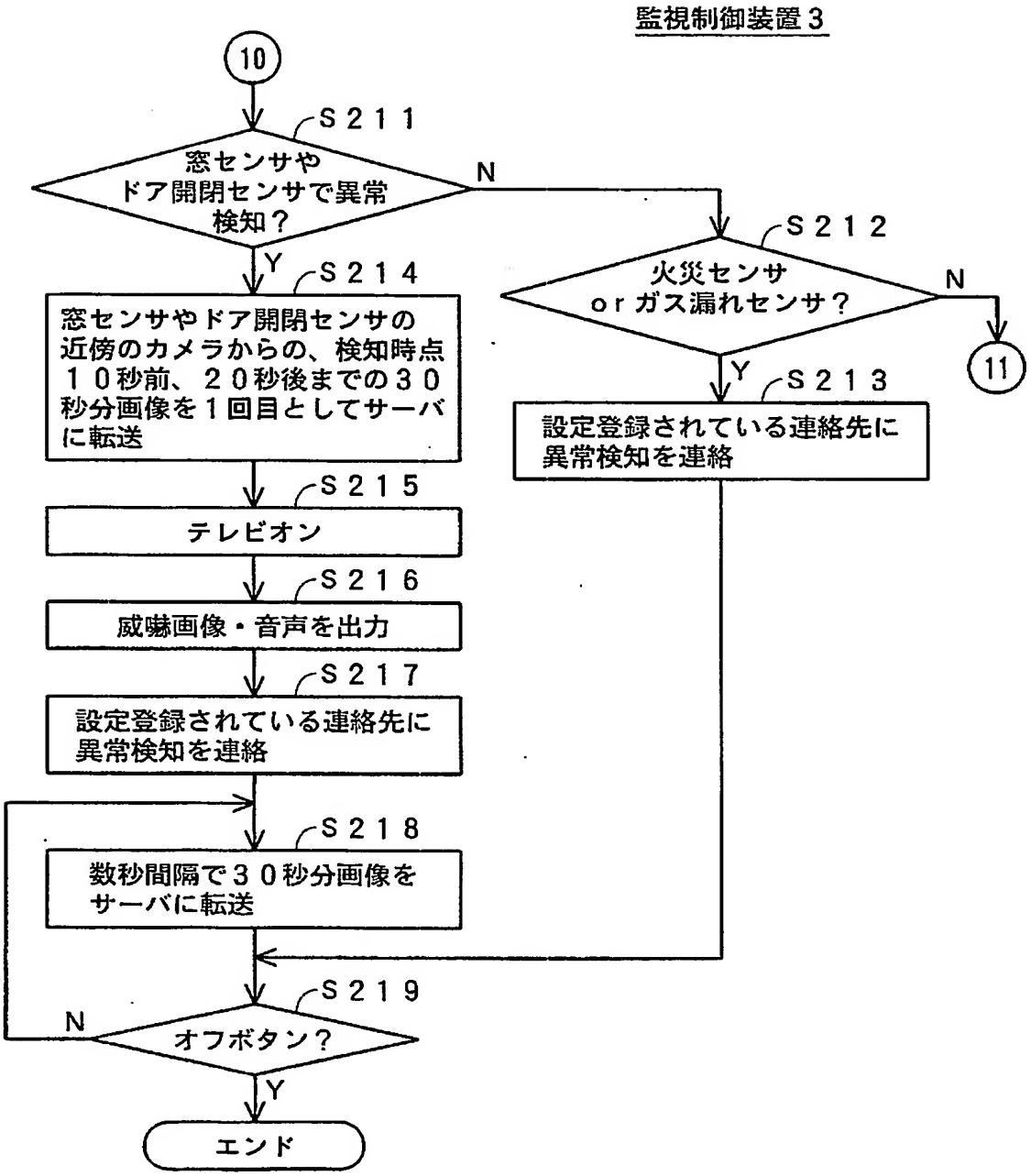
【図２６】


監視制御装置３
スタート
Ｓ１７１
操作入力有？
N
Y
Ｓ１７２
セキュリティボタン？
N
Y
Ｓ１７３
テレビオン
Ｓ１７４
セキュリティモードオンの確認画面を表示
Ｓ１７５
テレビオートオフ
Ｓ１７６
所定時間経過？
N
Y
Ｓ１７７
セキュリティモードをオン
Ｓ１７８
セキュリティ監視動作
Ｓ１７９
オフボタン？
N
Y
その他の処理
Ｓ１８０
Ｓ１８１
テレビオン
Ｓ１８２
セキュリティモードオフの確認画面を表示
Ｓ１８３
テレビオートオフ
Ｓ１８４
セキュリティモードをオフにする

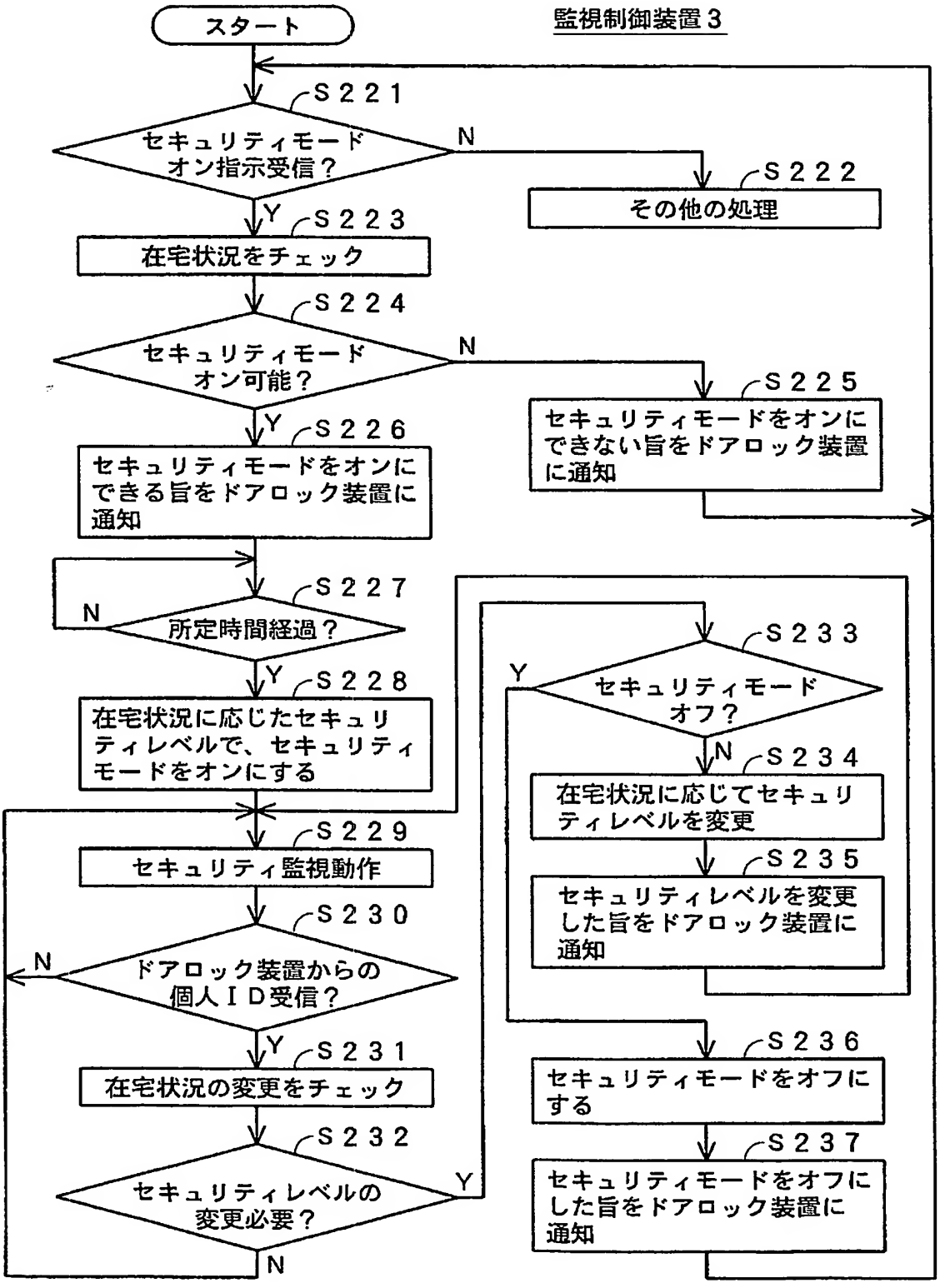
【図２７】


監視制御装置３
セキュリティモードオン
Ｓ１９１
カメラによる画像取り込み開始
Ｓ１９２
窓・ドア監視オン
Ｓ１９３
火災・ガス漏れ監視オン
11
Ｓ１９４
人感センサ
により侵入者検知？
N
Y
10
Ｓ１９５
照明オン
Ｓ１９６
検知時点の１０秒前、２０秒後までの３０秒分
画像を１回目としてサーバに転送
Ｓ１９７
テレビオン
Ｓ１９８
威嚇画像・音声を出力
Ｓ１９９
設定登録されている連絡先に異常検知を連絡
Ｓ２００
数秒間隔で３０秒分画像をサーバに転送
Ｓ２０１
人感センサ
非検知？
N
Y
Ｓ２０２
３０秒分画像の転送中止

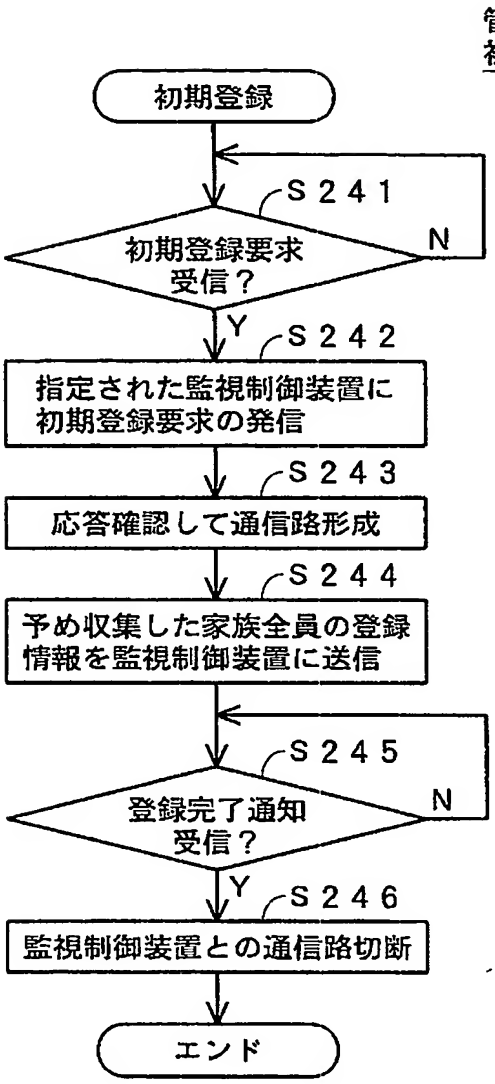
【図２８】


監視制御装置３
10
S２１１
窓センサや
ドア開閉センサで異常
検知？
N
Y
S２１２
火災センサ
ｏｒガス漏れセンサ？
N
Y
11
S２１３
設定登録されている連絡先に
異常検知を連絡
S２１４
窓センサやドア開閉センサの
近傍のカメラからの、検知時点
１０秒前、２０秒後までの３０
秒分画像を１回目としてサーバ
に転送
S２１５
テレビオン
S２１６
威嚇画像・音声を出力
S２１７
設定登録されている連絡先に
異常検知を連絡
S２１８
数秒間隔で３０秒分画像を
サーバに転送
S２１９
N
オフボタン？
Y
エンド

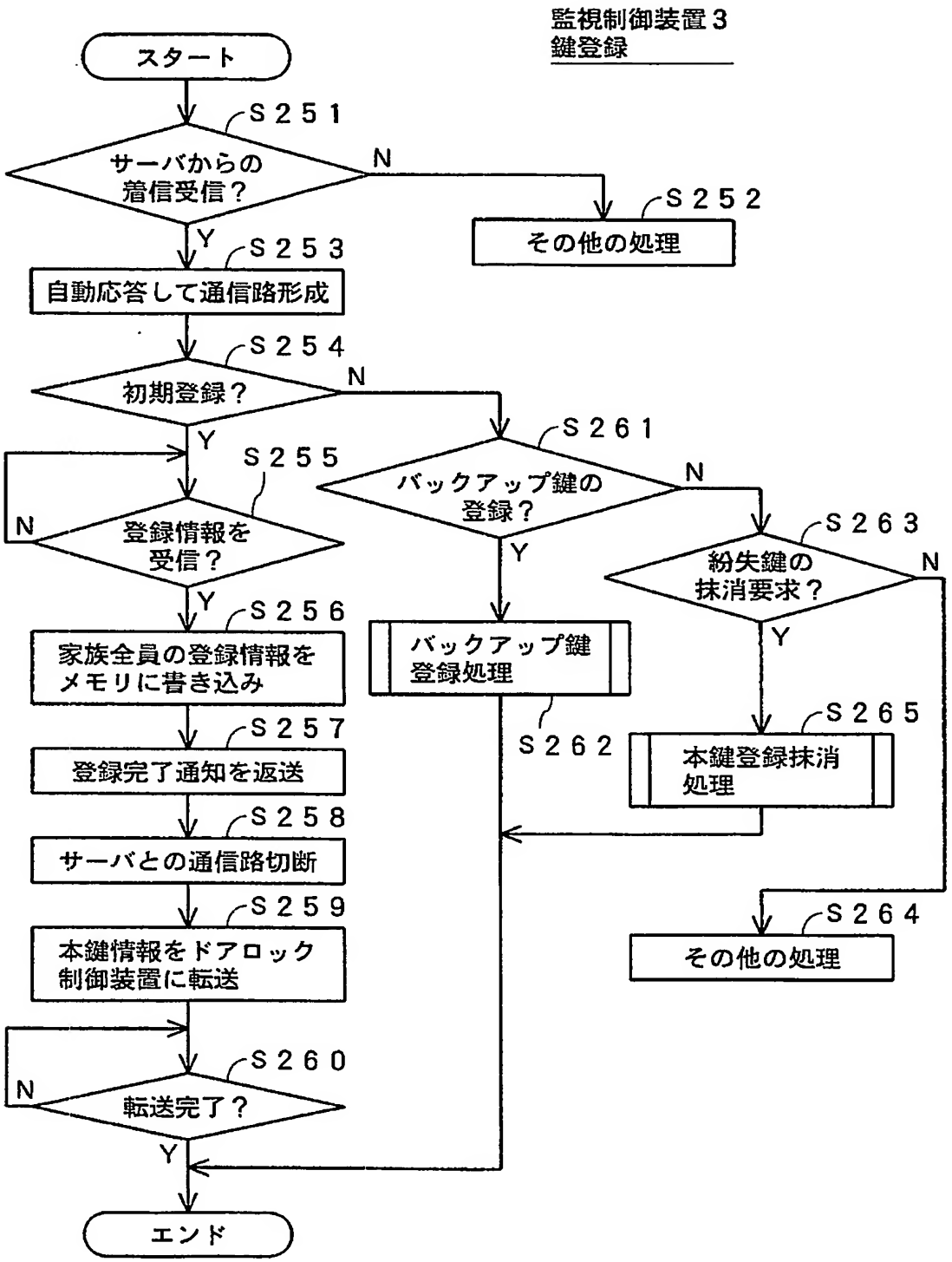
【図２９】


スタート
監視制御装置３
S２２１
セキュリティモードオン指示受信？
N
S２２２
その他の処理
Y
S２２３
在宅状況をチェック
S２２４
セキュリティモードオン可能？
N
S２２５
セキュリティモードをオンにできない旨をドアロック装置に通知
Y
S２２６
セキュリティモードをオンにできる旨をドアロック装置に通知
S２２７
N
所定時間経過？
Y
S２２８
在宅状況に応じたセキュリティレベルで、セキュリティモードをオンにする
S２２９
セキュリティ監視動作
S２３０
N
ドアロック装置からの個人ＩＤ受信？
Y
S２３１
在宅状況の変更をチェック
S２３２
セキュリティレベルの変更必要？
Y
N
S２３３
Y
セキュリティモードオフ？
N
S２３４
在宅状況に応じてセキュリティレベルを変更
S２３５
セキュリティレベルを変更した旨をドアロック装置に通知
S２３６
セキュリティモードをオフにする
S２３７
セキュリティモードをオフにした旨をドアロック装置に通知

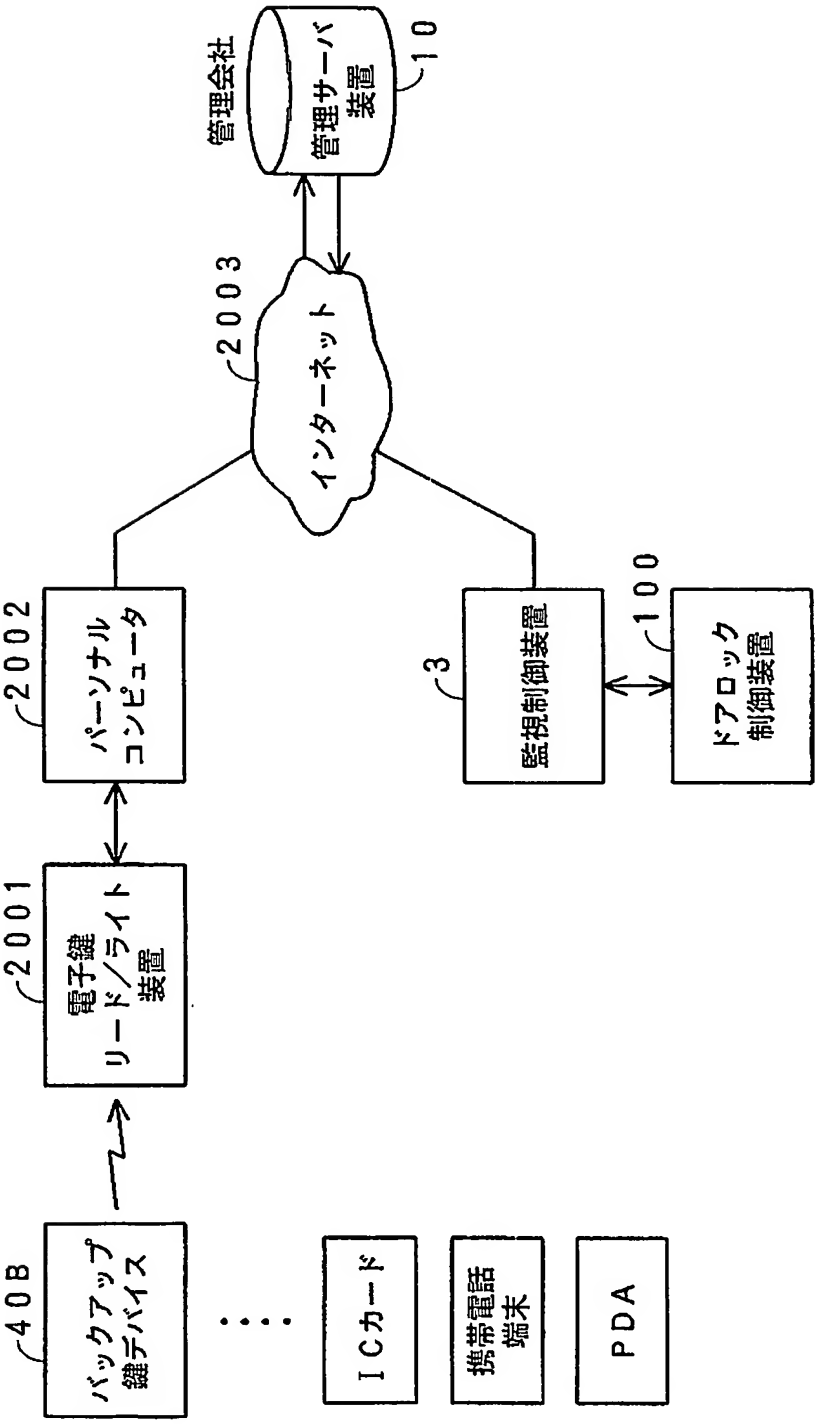
【図３０】


管理サーバ装置１０
初期登録
初期登録
Ｓ２４１
初期登録要求
受信？
N
Y
Ｓ２４２
指定された監視制御装置に
初期登録要求の発信
Ｓ２４３
応答確認して通信路形成
Ｓ２４４
予め収集した家族全員の登録
情報を監視制御装置に送信
Ｓ２４５
登録完了通知
受信？
N
Y
Ｓ２４６
監視制御装置との通信路切断
エンド

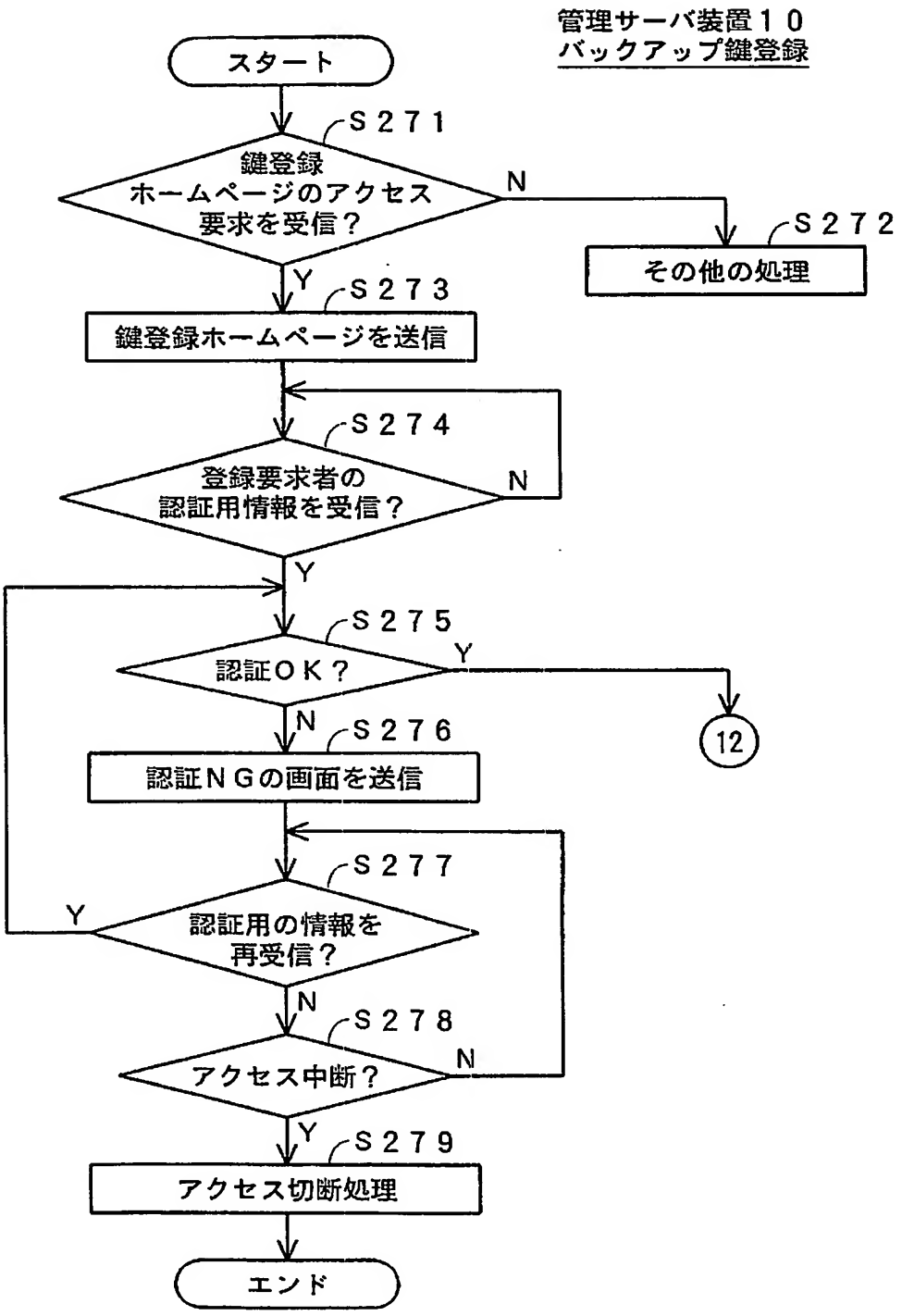
【図３１】


監視制御装置３
鍵登録
スタート
Ｓ２５１
サーバからの着信受信？
N
Ｓ２５２
その他の処理
Y
Ｓ２５３
自動応答して通信路形成
Ｓ２５４
初期登録？
N
Y
Ｓ２５５
登録情報を受信？
N
Y
Ｓ２５６
家族全員の登録情報をメモリに書き込み
Ｓ２５７
登録完了通知を返送
Ｓ２５８
サーバとの通信路切断
Ｓ２５９
本鍵情報をドアロック制御装置に転送
Ｓ２６０
転送完了？
N
Y
エンド
Ｓ２６１
バックアップ鍵の登録？
N
Y
バックアップ鍵登録処理
Ｓ２６２
Ｓ２６３
紛失鍵の抹消要求？
N
Y
Ｓ２６５
本鍵登録抹消処理
Ｓ２６４
その他の処理

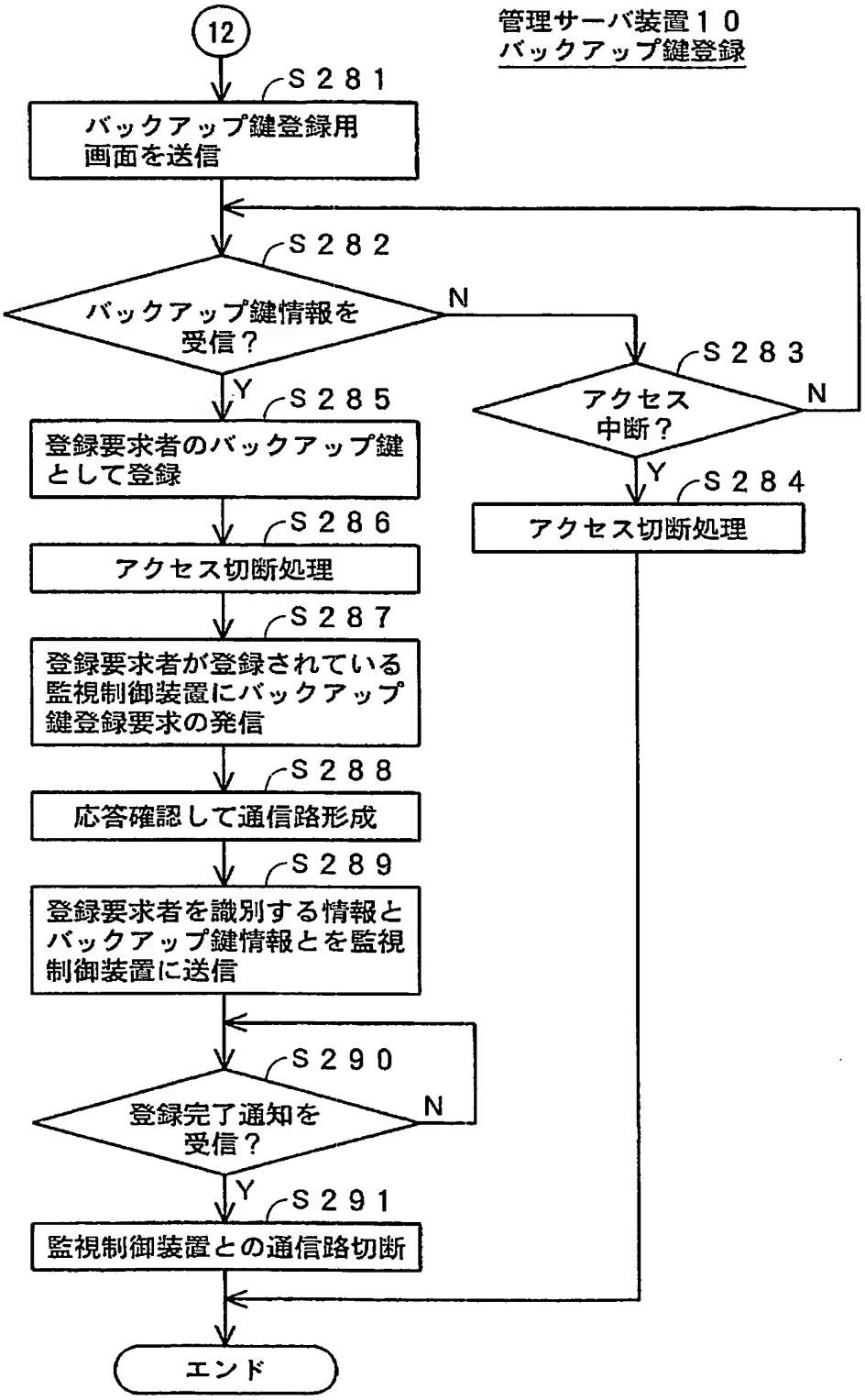
【図３２】


管理会社
管理サーバ装置
10
2003
インターネット
2002
パーソナルコンピュータ
3
監視制御装置
100
ドアロック制御装置
2001
電子鍵リード／ライト装置
40B
バックアップ鍵デバイス
ICカード
携帯電話端末
PDA

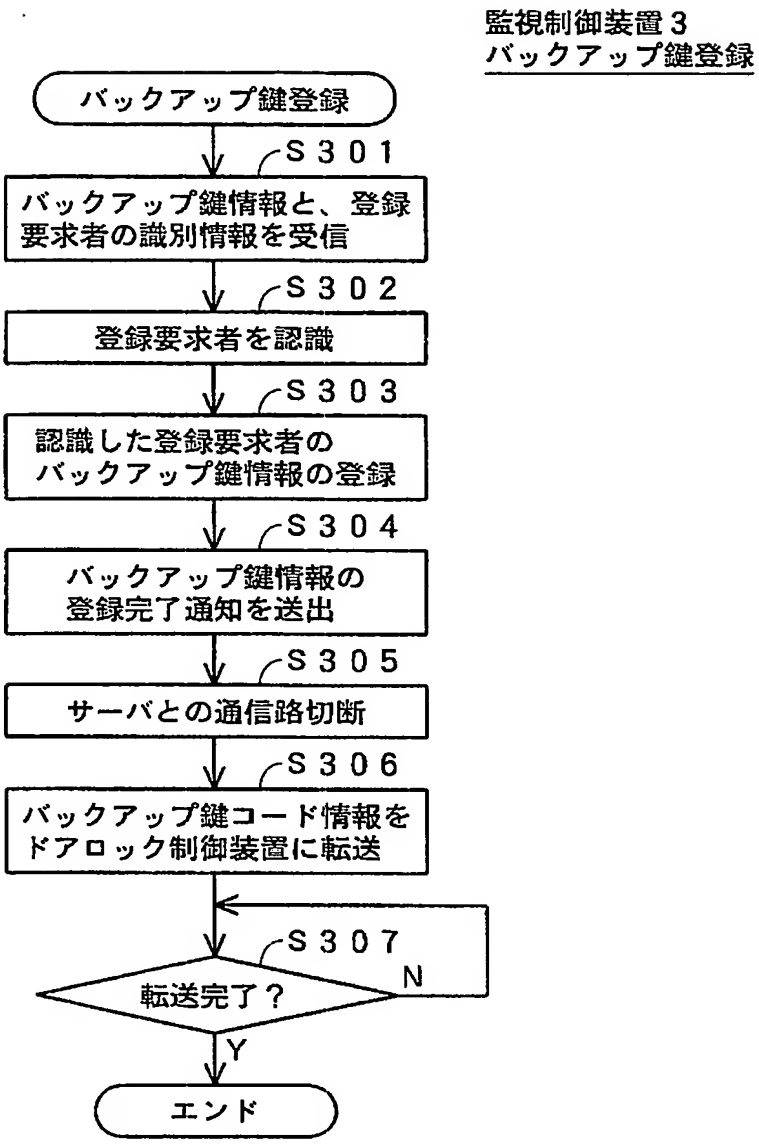
【図３３】


管理サーバ装置１０
バックアップ鍵登録
スタート
Ｓ２７１
鍵登録
ホームページのアクセス
要求を受信？
N
Ｓ２７２
その他の処理
Y
Ｓ２７３
鍵登録ホームページを送信
Ｓ２７４
登録要求者の
認証用情報を受信？
N
Y
Ｓ２７５
認証ＯＫ？
Y
12
N
Ｓ２７６
認証ＮＧの画面を送信
Ｓ２７７
認証用の情報を
再受信？
Y
N
Ｓ２７８
アクセス中断？
N
Y
Ｓ２７９
アクセス切断処理
エンド

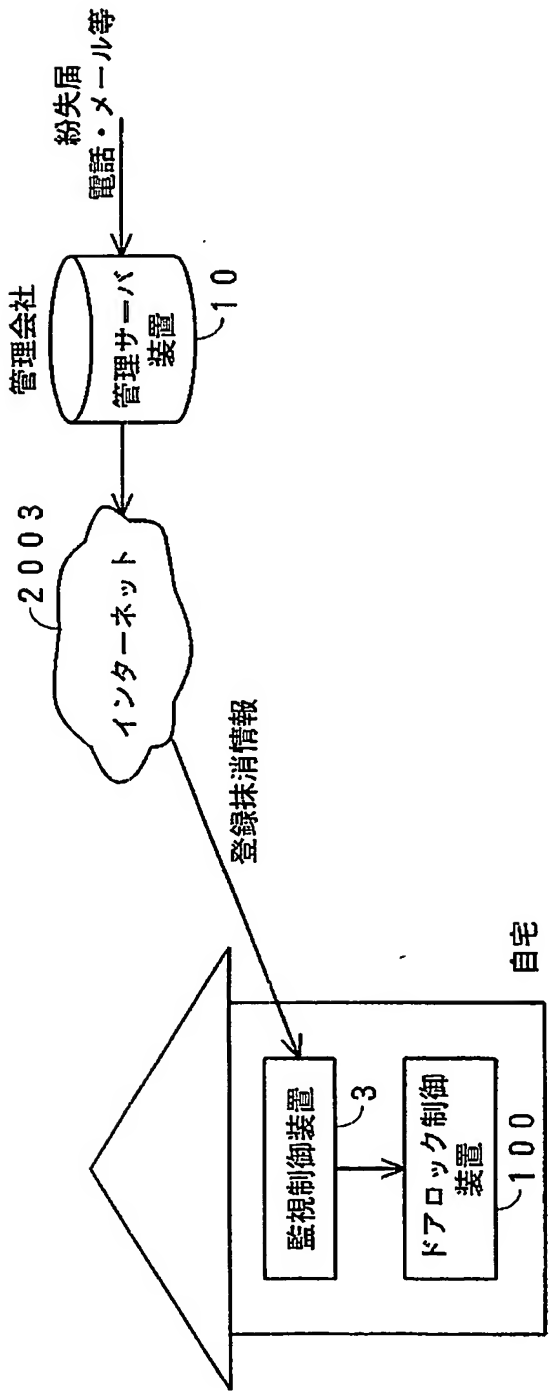
【図３４】


管理サーバ装置１０
バックアップ鍵登録
12
S２８１
バックアップ鍵登録用
画面を送信
S２８２
バックアップ鍵情報を
受信？
N
Y
S２８３
アクセス
中断？
N
Y
S２８４
アクセス切断処理
S２８５
登録要求者のバックアップ鍵
として登録
S２８６
アクセス切断処理
S２８７
登録要求者が登録されている
監視制御装置にバックアップ
鍵登録要求の発信
S２８８
応答確認して通信路形成
S２８９
登録要求者を識別する情報と
バックアップ鍵情報とを監視
制御装置に送信
S２９０
登録完了通知を
受信？
N
Y
S２９１
監視制御装置との通信路切断
エンド

【図３５】

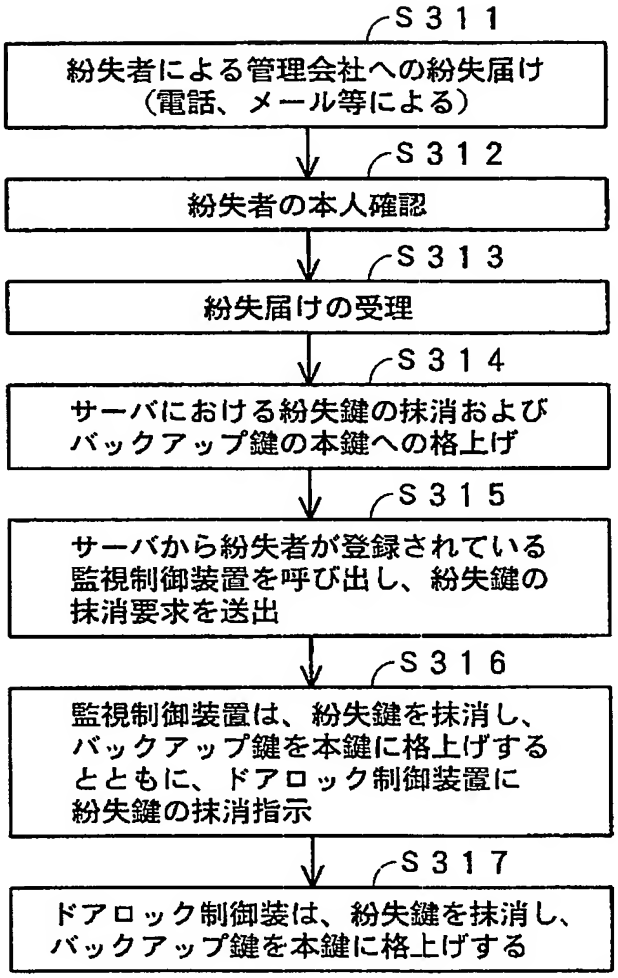

監視制御装置３
バックアップ鍵登録
バックアップ鍵登録
Ｓ３０１
バックアップ鍵情報と、登録要求者の識別情報を受信
Ｓ３０２
登録要求者を認識
Ｓ３０３
認識した登録要求者のバックアップ鍵情報の登録
Ｓ３０４
バックアップ鍵情報の登録完了通知を送出
Ｓ３０５
サーバとの通信路切断
Ｓ３０６
バックアップ鍵コード情報をドアロック制御装置に転送
Ｓ３０７
転送完了？
N
Y
エンド

【図３６】

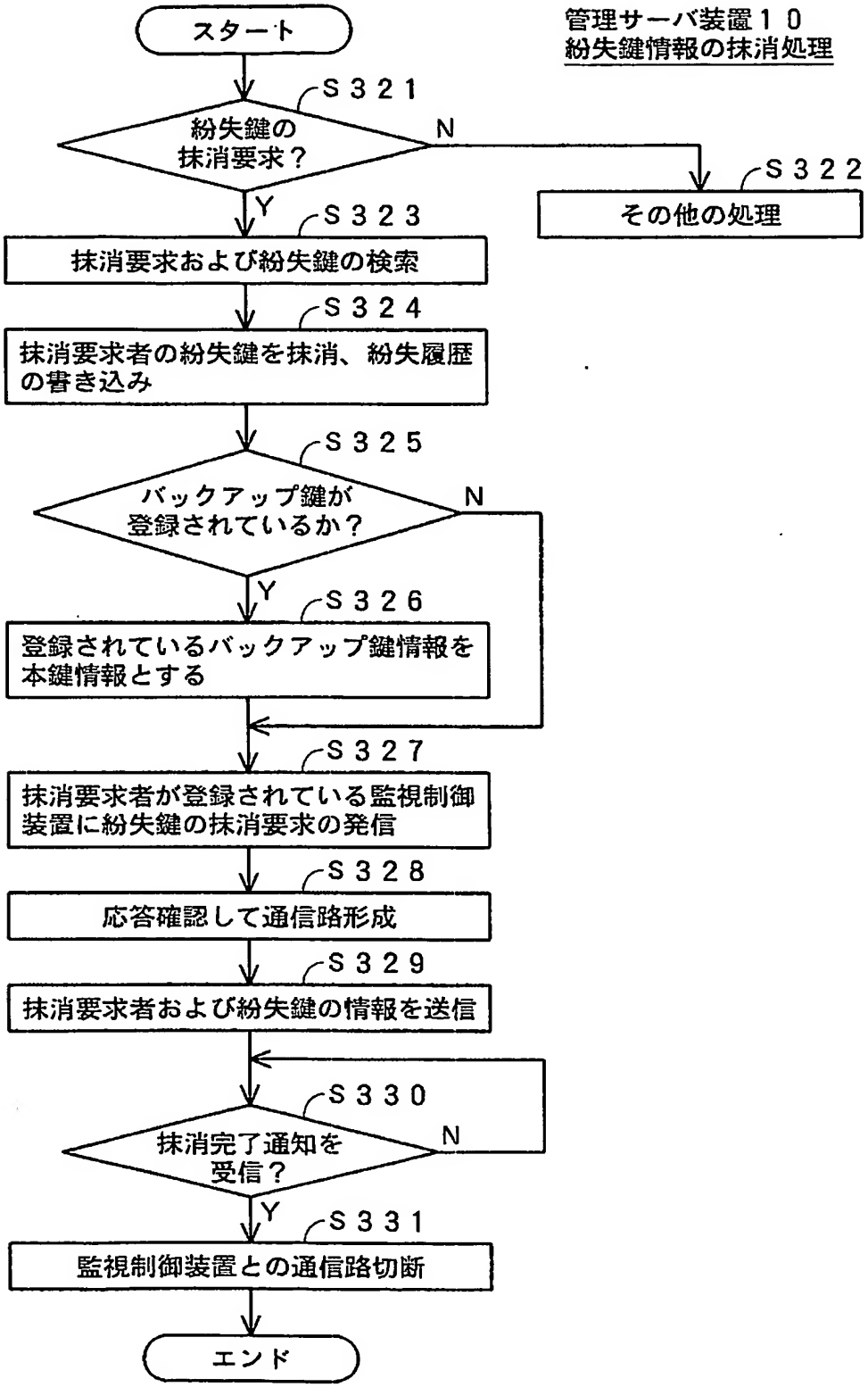

紛失届
電話・メール等
管理会社
管理サーバ
装置
10
2003
インターネット
登録抹消情報
自宅
監視制御装置
3
ドアロック制御
装置
100

【図３７】

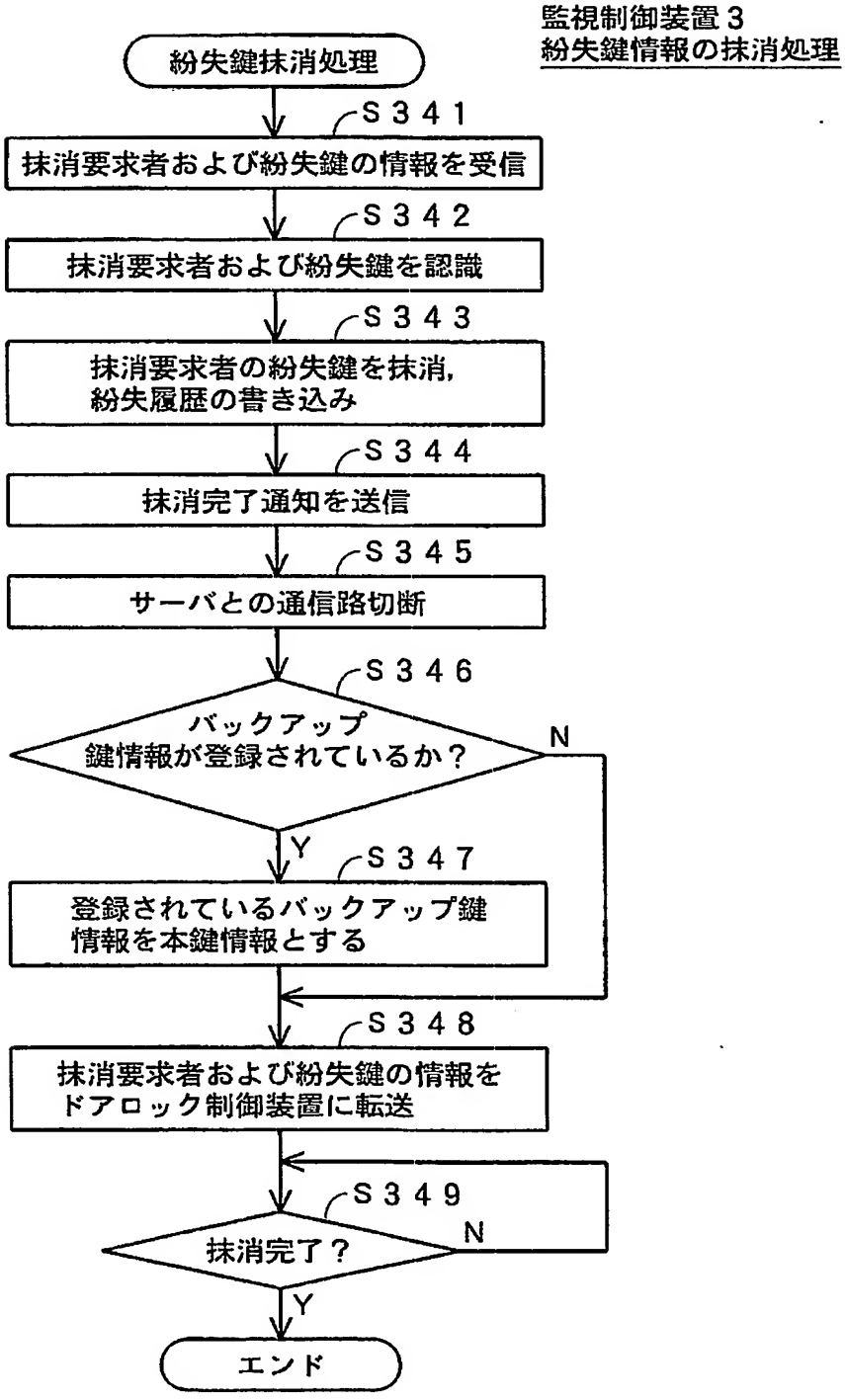
紛失鍵の抹消手順



【図３８】


スタート
管理サーバ装置１０
紛失鍵情報の抹消処理
Ｓ３２１
紛失鍵の
抹消要求？
N
Ｓ３２２
その他の処理
Y
Ｓ３２３
抹消要求および紛失鍵の検索
Ｓ３２４
抹消要求者の紛失鍵を抹消、紛失履歴
の書き込み
Ｓ３２５
バックアップ鍵が
登録されているか？
N
Y
Ｓ３２６
登録されているバックアップ鍵情報を
本鍵情報とする
Ｓ３２７
抹消要求者が登録されている監視制御
装置に紛失鍵の抹消要求の発信
Ｓ３２８
応答確認して通信路形成
Ｓ３２９
抹消要求者および紛失鍵の情報を送信
Ｓ３３０
抹消完了通知を
受信？
N
Y
Ｓ３３１
監視制御装置との通信路切断
エンド

【図３９】


監視制御装置３
紛失鍵情報の抹消処理
紛失鍵抹消処理
Ｓ３４１
抹消要求者および紛失鍵の情報を受信
Ｓ３４２
抹消要求者および紛失鍵を認識
Ｓ３４３
抹消要求者の紛失鍵を抹消，
紛失履歴の書き込み
Ｓ３４４
抹消完了通知を送信
Ｓ３４５
サーバとの通信路切断
Ｓ３４６
バックアップ
鍵情報が登録されているか？
N
Y
Ｓ３４７
登録されているバックアップ鍵
情報を本鍵情報とする
Ｓ３４８
抹消要求者および紛失鍵の情報を
ドアロック制御装置に転送
Ｓ３４９
抹消完了？
N
Y
エンド

【書類名】　要約書

【要約】

【課題】　電子鍵管理に関してセキュリティが高い通信システムを提供する。

【解決手段】　電子鍵情報に応じてドアの施錠、開錠を行なうためのドアロック機構を制御する制御装置と、前記制御装置に前記電子鍵情報を送信する通信装置とからなる通信システムである。通信装置は、同一のものが存在しないように一元管理されて割り振られた識別情報を記憶する第１の記憶部を備え、第１の通信部を介して、第１の記憶部の識別情報を、ドアの施錠、開錠を制御するための電子鍵情報として制御装置に送信する。制御装置は、電子鍵情報としての識別情報を記憶する第２の記憶部と、第２の記憶部に識別情報を電子鍵情報として登録するための登録手段と、第２の通信部を通じて通信装置から受信した識別情報と、第２の記憶部に記憶されている識別情報とを比較し、その比較結果に基づいてドアの施錠、開錠を制御する第２の制御部とを備える。

【選択図】　図１

特願２００２－２７８４３６

出願人履歴情報

識別番号　［０００００２１８５］

１．変更年月日　１９９０年　８月３０日
［変更理由］　新規登録
住　所　東京都品川区北品川６丁目７番３５号
氏　名　ソニー株式会社